

THE WIRELESS HACKER PROJECT

802.11 Security

graduation paper

```
Starting nmap V. 2.54BETA29 ( www.insecure.org/nmap/ )
Interesting ports on local host (127.0.0.1):
(The 1539 ports scanned by nmap are in state: closed)
Port      State      Service
21/tcp    open      Ftp
22/tcp    open      ssh
23/tcp    open      telnet
80/tcp    open      http
113/tcp   open      auth
515/tcp   open      printer
1241/tcp  open      msrpc
3001/tcp  open      nmap
6000/tcp  open      X11
```



Matthieu B. Pâques
Eddie Michiels, Carel van Leeuwen, Ing Widya
department of Computer Science, APS group
University of Twente, November 2004

THE WIRELESS HACKER PROJECT

802.11 Security

graduation paper

Matthieu B. Pâques

Graduation committee:

Eddie Michiels
Carel van Leeuwen
Ing Widya

Application Protocol Systems chair
Department of Computer Science
University of Twente

Enschede, November 2004

Executive summary

The objective of this project is *to obtain insight in the vulnerabilities of WLAN security, in particular the security of the Utwente WLAN, and provide recommendations to remove or mitigate these vulnerabilities.*

I used the first part of the project to found out as much as possible on WLAN security. Subsequently I experimented with the most common attack tools to become familiar with their possibilities and methods. Based on this preliminary investigation I created the following list of threats to wireless networks.

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Interception and disclosure of sensitive information that is transmitted between two wireless devices.
- Denial of Service attacks at wireless connections or devices.
- Identity capture of legitimate users and subsequent use for illicit access on corporate networks.
- Theft of handheld devices leading to the disclosure of sensitive information.

With regard to security measures I concluded the following:

Basic security measures like WEP and MAC-filtering are weak and don't provide the degree of security most people expect. More advanced solutions are often expensive and time-consuming to deploy. Examples of these advanced techniques are VPN and 802.1x. When implemented in the right way, these techniques offer an acceptable level of security for most purposes, but still contain certain vulnerabilities. The state-of-the-art solution 802.1i solves most of these remaining vulnerabilities.

Based on the gained experience I designed two series of penetration tests to uncover these weaknesses in practice. The results of these tests and recommendations based on these tests can be summarized as follows:

The threats and vulnerabilities of WLANs are often underestimated or unknown especially for SOHO networks. Approximately 60% of the personal WLANs detected are badly configured, using a weak protection technique or have no protection in place at all. Users of the Utwente WLAN (protected using the 802.1x technology) are well protected against outsiders, but not to certain attacks from other internal users. In general the implemented security facilities of the Utwente WLAN left a good impression. Nevertheless I make some recommendations. Various security procedures aren't documented and depend on the experience of administrators. I recommend documenting all important procedures. Another recommendation concerns the password policy for users. Users are not forced to change their passwords with regular intervals or to use a defined difficulty level. The last recommendation concerns the use of an intrusion detection system to protect users against each other. .

This paper provides insight in the vulnerabilities of WLAN security, in particular the security of the Utwente WLAN and provides recommendations to remove or mitigate these vulnerabilities.

Preface

During my internship I gained experience with computer security. I got interested and decided to choose my main subject in the same direction. The UT had recently implemented a whole new WLAN on the campus of the University. Since I didn't have the opportunity to learn more about wireless security in particular before, I asked the UT, whether there was a possibility to choose this subject for my graduation paper. The UT created an assignment on this subject which can be found in appendix 7.

There are a lot wireless technologies available: Bluetooth, Infrared, HomeRF, WiFi, 802.11a, UMTS, GPRS and more. During this project I noticed that it was important to define the scope of the subject from the beginning.

A lot of WLAN's today contain vulnerabilities unknown by the owners. These vulnerabilities are often caused by badly installed systems or already dated hard- or software. Besides, attacks on wireless LAN's are evolving with the same speed as the technology itself. Therefore yesterdays secure implementation could be at risk today.

This paper should provide a better insight in the vulnerabilities of WLAN security, in particular the security of the Utwente WLAN and provide recommendations to remove or mitigate these vulnerabilities.

I want to thank Eddie Michiels and Carel van Leeuwen for their support during this project. I also want to thank Sander Smit, Gert Meijerink and Erik Nijboer from the ITBE-staff for participating in the interviews and lending me the necessary equipment.

During this project, I did not only learn a lot about wireless technologies, but also came into contact with legislation issues and techniques as social engineering. I never regretted the choice of this subject and can make good use of the gained experience in the future. I really enjoyed solving the 'puzzles' in the attacks and hope this enthusiasm can be derived from this paper.

Matthieu Pâques

Enschede November 2004

Contents

1	Introduction	8
1.1	Project objective and research questions	9
1.2	Hypothesis	10
1.3	Project procedure	10
1.4	Scope and limitations	11
1.5	Related projects	12
1.6	How to read this paper	12
2	Preliminary investigation	13
2.1	Basic 802.11 security	15
2.2	Known attacks and tools	20
2.2.1	Different types of attacks	20
2.2.2	Short description of useful security and attack tools	31
2.3	Advanced wireless security techniques	32
2.3.1	VPN	32
2.3.2	WEB based access and hotspot security	35
2.3.3	The IEEE 802.1x standard	38
2.4	Legal provisions and requirements	44
2.5	The Utwente WLAN	45
2.5.1	Management measures	46
2.5.2	Operational measures	46
2.5.3	Technical measures	46
2.5.4	Knows security issues on this implementation	48
2.6	Under development (state-of-the-art solutions)	49
2.6.1	Temporal Key Integrity Protocol (TKIP)	49
2.6.2	Wifi Protected Access (WPA)	51
2.6.3	802.11i (WPA2)	51
2.7	Summary	51
3	Weaknesses of the wireless network	52
3.1	Attacks on a wireless network	52
3.2	Pentests vol. 1: A quick wardrive session	53
3.2.1	Preparing for the pentests	54
3.2.2	Phase 1: Reconnaissance	54
3.2.3	Phase 2: Scanning	56
3.2.4	Phase 3, 4 and 5: Access to the WLAN	59
3.3	Pentests vol. 2: Attacks on the Utwente WLAN	61
3.3.1	Preparing for the pentests	61
3.3.2	Phase 1: Reconnaissance	61
3.3.3	Phase 2: Scanning	62
3.3.4	Phase 3, 4 and 5: Access to the WLAN	63
3.4	Summary	72
4	The Utwente security- policy and measures	73
4.1	SNT (Studenten Net Twente)	73
4.2	ITBE	74
4.3	Summary	74

5	Countermeasures	75
5.1	Countermeasures	75
5.1.1	Applicability of the countermeasures	75
5.1.2	Management Countermeasures	75
5.1.3	Operational Countermeasures	76
5.1.4	Technical Countermeasures	77
5.1.5	Measures against specific attack types	78
5.2	Intrusion Detection Systems (IDS) and monitoring	80
5.3	Auditing	80
5.4	Summary	81
6	Conclusion, evaluation and recommendations	82
6.1	Conclusion, evaluation and recommendations	82
6.2	Subjects suggested by the author for further research	83
7	References	84
8	Glossary	88
8.1	Acronyms and Abbreviations	89
	Appendices	92
	Appendix 1: Eisen en wensen aan het WLAN mbt de beveiliging	92
	Appendix 2: Basisconfiguratie acces point UT WLAN	94
	Appendix 3: Wardriving	95
	Appendix 4: Examples of detected AP's with default passwords	97
	Appendix 5: Authentication procedure on the 802.1X network.	98
	Appendix 6: Vragen aan het ITBE	100
	Appendix 7: Opdrachtschrijving afstudeeropdracht	105

List of tables

Table 1: Legal provisions concerning computer crime	44
Table 2: WLAN division.....	45
Table 3: Detected SSIDs on the campus	55
Table 4: Access point configuration.....	66

List of figures

Figure 1: WLAN on the University.....	8
Figure 2: User segmentation without VLANs.....	14
Figure 3: WEP encipherment	16
Figure 4: A WEP packet.....	16
Figure 5: Client states.....	18
Figure 6: MiTM attack	22
Figure 7: Setting up a connection.....	23
Figure 8: Session hijacking in detail	23
Figure 9: A MiTM attack scenario.....	24
Figure 10: ARP attack against two wireless clients	25
Figure 11: Capturing a packet	26
Figure 12: Reinjecting the captured packet.....	26
Figure 13: Network settings	26
Figure 14: 802.1x elements	38
Figure 15: EAP over LAN	39
Figure 16: Entities in EAP authentication.....	39
Figure 17: Authentication messages between client and authenticator.....	40
Figure 18: Authentication of a client.....	41
Figure 19: An EAP packet	42
Figure 20: Network structure	45
Figure 21: Access point placement on the campus	46
Figure 22: Cisco Aironet 1200 Series Access Points.....	47
Figure 23: The Cisco catalyst 6500 switch	47
Figure 24: Radius proxy	48
Figure 25: Key generation with TKIP.....	49
Figure 26: WEP encrypted packet.....	50
Figure 27: WEP encrypted packet with TKIP.....	50
Figure 28: Access points in Enschede.....	53
Figure 29: Access point in Enschede in detail	53
Figure 30: Kmac spoofs our MAC-address.....	54
Figure 31: Detected access points with Netstumbler	55
Figure 32: Signal strength measurement in Netstumbler	56
Figure 33: Sniffing packets with Kismet.....	57
Figure 34: Network details from Kismet.....	57
Figure 35: Examining the captured packets with Ethereal.....	58
Figure 36: Subnet scanning with Look@LAN.....	58
Figure 37: Portscanning with NMap	59
Figure 38: Searching for vulnerabilities with LanGuard	59
Figure 39: Admin shares victims system	60
Figure 40: Network details from winXP	62
Figure 41: MitM attack	64
Figure 42: CLI settings.....	67
Figure 43: My 'ITBE id card'	67
Figure 44: rogue access point.....	68
Figure 45: Linksys settings	69
Figure 46: Detailed settings for the Linksys card	69
Figure 47: First ARP poisoning on the LAN	71
Figure 48: Retrieving user credentials using ARP spoofing	72

1 Introduction

In this chapter I describe the project objective and the research questions. I also describe the followed procedure and related projects. The chapter concludes with some reading instructions.

Wireless local area networks (WLANs) are quickly becoming popular. Most important causes for this popularity are convenience and costs. WLANs require security facilities different from those applied in a wired environment. Basic security like WEP-encryption or MAC-filtering is weak and there exist already easy to use tools to bypass these measures.

As a result companies have to adapt to the quickly changing threats and update to a new security solution. Possible solutions are VPN, or the new 802.1x standard.

The University of Twente has deployed an extended high speed WLAN for students and employers. The wireless network spreads both the apartments as the faculties on the Utwente area. An indication of the covered area is shown below.

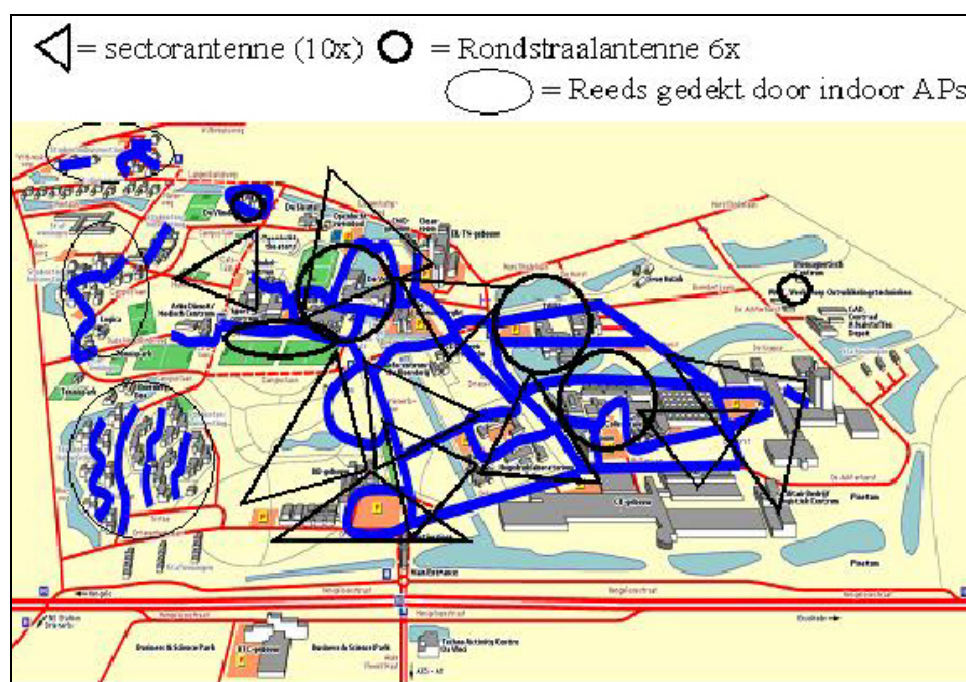


Figure 1: WLAN on the University

The network consists of 650 Cisco 1200 series access points, and a RADIUS authentication server. The LDAP server (used for storing email account information) provides account information to the RADIUS server. The same account is used for both the wireless network as well as access to the email boxes and ftp directory of all students. This network is protected using the new 802.1x technology.

The UT has mentioned the requests with respect to the security below in determining the final implementation [COOK]

- *Figurative usage should be resisted*
- *Eavesdropping and authentication have to be arranged in a adequate manner*

In a presentation [WLUS] about the WLAN security by Sander Smit of the UT the demands below are enumerated (translated from Dutch):

- *Unique identification of the user*
- *Identity theft should be impossible*
- *Central registration of users*
- *Guest usage should be easily possible*
- *Automatic VLAN assignment*

The usage of words like ‘resisted’ or ‘adequate’ is not very concrete. Unfortunately no other information about the demands on the security of the WLAN is available. Furthermore there is no detailed information about the other aspects that were considered (e.g. costs and ease of use) to determine the preferred security level also. Therefore I based my project questions on the assumption the goal of the implementation is to make figurative usage and eavesdropping as difficult as possible i.e. for both outsiders as well as other users of the WLAN with a valid account and verified this assumption in an interview with ITBE staff in a later stage of the project.

1.1 Project objective and research questions

The objective of this project is *to obtain insight in the vulnerabilities of WLAN security, in particular the security of the Utwente WLAN and provide recommendations to remove or mitigate these vulnerabilities*. This work should provide answers to the following questions:

General questions

- What are the basic 802.11 security options?
- What are the known problems with these security options, for example WEP weaknesses?
- What are the additional or alternative techniques for the 802.1 security (including state-of-the-art solutions) and what is the level of security these additional techniques provide?
- What does a common attack on a WLAN look like?
- Which tools are available for attacks on WLANs?

Questions about the Utwente WLAN

- What are the demands of the UT on the WLAN security?
- What is the current implementation that should take care of these demands (technology, hardware, IDS usage, policies and responsibilities)?
- Are these demands realized using the current implementation?
- If not, what are the vulnerable parts in the wireless network that request attention?
- What are the possible risks if the network is compromised?
- Are there known security problems with the chosen implementation (for example with hardware, software or physical protection)?
- And finally, how can the present security be improved?

1.2 Hypothesis

In this project I distinguish two different hypotheses. The first one concerns WLAN security in general. The second one concerns the implementation of the WLAN at the University of Twente.

WLAN technology is changing quickly. Wireless products on the market today are hardly tested and often installed with default settings. Based on this my hypothesis concerning wireless security in general becomes:

Most of the WLAN vulnerabilities today are caused by badly installed systems or already dated hard- or software. Unaware users are the biggest threat to the wireless network.

The UT has chosen to use the new 802.1x technology to protect the wireless network. The use of this technology prevents a large number of the current security problems. Given the fast developments in this area I expect however that the present implementation will contain some security vulnerabilities.

The UT has two important demands on the WLAN security as indicated before.

- Figurative usage should be resisted
- Eavesdropping and authentication have to be arranged in a adequate manner

My hypothesis below has been based on the expectation as well as these demands.

The protection of the wireless network of the UT contains vulnerabilities which can be abused with sophisticated techniques. As a result unauthorized access to the network and/or disclosure of sensitive data is possible and therefore the demands of the UT on the WLAN security are not met.

1.3 Project procedure

This paragraph gives a step-by-step description of the research procedure:

Rough determination of the aim, research questions, and scope of the project

In this stage I roughly defined the aim and scope of the subject and created the list of research questions based on the project objective (1.1).

Preliminary investigation

I used the first part of the project to collect information from several sources including but not limited to the Internet (websites, forum discussions), papers, books and articles.

Subsequently I experimented with the most common tools to become familiar with their possibilities and methods. At this moment I created the list of possible shortcomings based on the results of the preliminary investigation

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Interception and disclosure of sensitive information that is transmitted between two wireless devices.
- Denial of Service attacks at wireless connections or devices.
- Identity capture of legitimate users and subsequent use for illicit access on corporate networks.
- Theft of handheld devices leading to the disclosure of sensitive information.

Final determination of the aim, research questions, and scope of the project

Based on the results of the preliminary investigation, I determine the final aim, research questions and scope of the project in this stage.

Design of two series of penetration tests

In this stage designed two series of penetration tests to uncover these weaknesses.

The first series are aimed at some WLANs I detected in the area. Most networks were protected with basic security techniques.

The second series were aimed at the University WLAN. Because of the different approach to the attack for people with- or without an account to enter the LAN I distinguish students (with a valid account) and outsiders (possibly using the guest network) here.

Execution of the penetration test, processing and verification of the test results.

The tests are executed in this stage. The results of the project are discussed with the technical staff of the University (ITBE) responsible for the WLAN. In this way I could inform them of my results and recommendation and at the same time verify my results and obtain additional information. The recommendations and conclusion of the project are based on the read documents, project results and interviews with ITBE staff.

Evaluation, conclusion and reporting

During the project I had periodical meetings with my supervisors to evaluate the progress, the made choices and discuss the results and planning. In this phase I create recommendation to secure a wireless LAN. This paper was created during the different stages of the project. This project contains next to different subjects information about the progress of the project and project in general. At the end of the project I will evaluate the project as a whole.

Preparation for the presentation

The presentation is prepared in this stage. This includes the preparation of sheets, inviting guest and taking care of a location.

Presentation

The final stage is the presentation of the project.

Obviously the privacy of the clients on the wireless network had to be respected during this project and therefore some rules were observed. For example I stored all sensitive project data in a protected (encrypted) bin and wiped all sensitive data after finishing the project.

1.4 Scope and limitations

The project aims at 802.11-security. Bluetooth, Infrared, HomeRF, WiFi, 802.11a, UMTS, GPRS and other wireless techniques fall out of the scope of this project.

This paper should not be distributed or multiplied without permission of the author.

1.5 Related projects

Hof, J.v.h., *Heterogeneous Network Access Security*, University Twente, May 2004
This paper gives an overview on the different types of security for wireless techniques as WLAN, UMTS and more.

Dekkers, P., *802.1X bij Surfnet, beveiliging op wireless en wired LAN*, [PAU] afstudeerverslag mei 2003, Hogeschool van Utrecht, Mei 2003,
This paper focuses on the possibilities of 802.1X and combination with different types of hardware and authentication methods. This paper is mainly theoretical, and focuses on the authentication method itself and not the end-to-end security which can contain the 802.1X method for authentication.

SURFnet, *pilot802.1x*. [PILO]
UT test on the security of their WLAN.

1.6 How to read this paper

This document covers details specific to wireless technologies and solutions. The document is technical in nature; however, it provides the necessary background to fully understand the topics that are discussed.

In *chapter 2* I describe the standard 802.11-security methods and known attacks as well as more advanced security techniques to protect a LAN against (most of) these attacks. I mention legal provisions briefly in the fourth paragraph. A description of the Utwente WLAN can be found in paragraph 2.5. The chapter concludes with an overview of the state-of-the-art solutions.

In *chapter 3* I describe the results of two series of penetration tests. The first one was performed in Enschede and shows how an insecure WLAN can be compromised. Next I focus on the 802.1x security solution chosen for the WLAN@UT project and perform six penetration tests here as well.

The results of the penetration tests on the University network are verified and discussed in *chapter 4*. Countermeasures to prevent or detect attacks on the WLAN are discussed in *chapter 5*. This paper concludes with a summary of the results, evaluation, final conclusion and possible recommendations for further projects as well as recommendations for the protection of WLANs in a particular environment including the Utwente WLAN (*chapter 6*).

A glossary, acronyms and abbreviations can be found in *chapter 8*

Because of the constantly changing nature of the wireless security industry and the threats and vulnerabilities to these technologies, readers are strongly encouraged to take advantage of other resources (including those listed in this document) for more current and detailed information.

2 Preliminary investigation

In this chapter I describe the results of the preliminary investigation. I give an overview of the basic WLAN security options and well known attacks and tools. I also describe more advanced security techniques which can be used in deploying an (almost) secure wireless network. The chapter concludes with a view on the state-of-the-art security techniques.

The preliminary investigation is based on the questions below.

General questions

- What are the basic 802.11 security options?
- What are the known problems with these security options like WEP weaknesses?
- What are the additional or alternative techniques for the 802.1 security and what is the level of security these additional techniques provide?
- What does a common attack on a WLAN look like?
- Which tools are available for attacks on WLANs?

Questions about the Utwente WLAN

- What are the demands of the UT on the WLAN security?
- What is the current implementation that should take care of these demands (used technology, hardware, IDS usage, policies)?

The remaining of this chapter provides answers to the questions above.

Ad-hoc and infrastructure mode

The IEEE 802.11 standard describes two different modes: *ad-hoc* mode and *infrastructure* mode. In *ad-hoc* mode all clients are connected directly with each other. In *infrastructure* mode all communication goes through a centralized access point (*access point*). The security techniques described below are based on clients operating in infrastructure mode unless indicated otherwise.

Virtual Local Area Networks (VLANs)

VLANs have the same attributes as physical LANs with the additional capability to group end stations to the same LAN segment regardless of the end stations' geographical location.

The concept of Layer 2 wired VLANs is extended to the WLAN with wireless VLANs. As with wired LANS, wireless VLANs define broadcast domains and segregate broadcast and multicast traffic between VLANs.

When VLANs are not used, an IT administrator must install additional WLAN infrastructure to segment traffic between user groups or device groups. For example, to segment traffic between employee and guest VLANs, an IT administrator must install two access points at each location throughout an enterprise WLAN network (as shown in *Figure 2*). However, with the use of wireless VLANs, one access point at each location can be used to provide access to both groups.

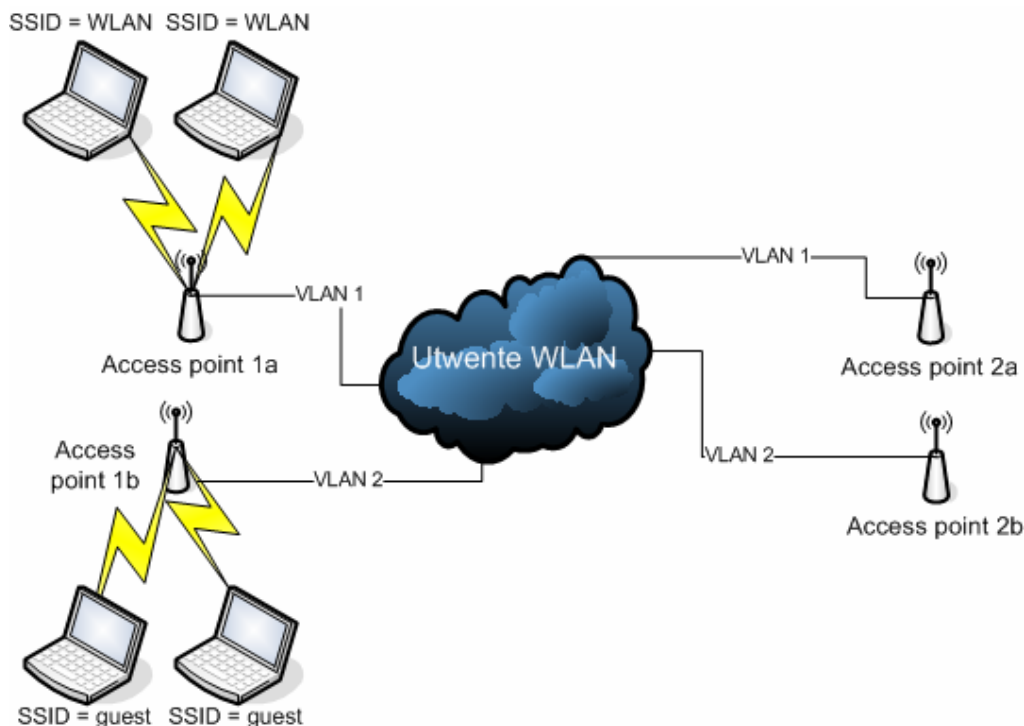


Figure 2: User segmentation without VLANs

A per-VLAN network security policy can be defined on the access point to allow the IT administrator to define appropriate restrictions per VLAN. The following parameters are configurable on the SSID wireless VLAN:

- SSID name: Configures a unique name per wireless VLAN
- Default VLAN ID: Default VLAN-ID mapping on the wired side
- Authentication types: Open, shared, and network-Extensible Authentication Protocol (EAP) types
- Media Access Control (MAC) authentication: Under open, shared, and network-EAP
- EAP authentication: Under open and shared authentication types
- Maximum number of associations: Ability to limit maximum number of WLAN clients per SSID

The following parameters are configurable on the wired VLAN side:

- Encryption key: This is the key used for broadcast and multicast traffic segmentation per VLAN. It is also used for static Wired Equivalent Privacy (WEP) clients (for both unicast and multicast traffic).
- Enhanced Message Integrity Check (MIC) verification for WEP: Enables MIC per VLAN.
- Temporal Key Integrity Protocol (TKIP): Enables per-packet key hashing per VLAN.
- WEP (broadcast) key rotation interval: Enables broadcast WEP key rotation per VLAN. This is only supported for wireless VLANs with IEEE 802.1X EAP protocols enabled (such as EAP Cisco Wireless [LEAP], EAP-Transport Layer Security [EAP-TLS], Protected Extensible Authentication Protocol [PEAP], and EAP-Subscriber Identity Module [EAP-SIM]).

- Default policy group: Applies policy group (set of Layer 2, 3, and 4 filters) per VLAN. Each filter (within a policy group) is configurable to allow or deny certain types of traffic.
- Default priority: Applies default class of service (CoS) priority per VLAN.

2.1 Basic 802.11 security

The four basic security mechanisms for 802.11 networks are:

- **MAC (Media Access Control)**
A wireless access points can verify the clients Media Access Control (MAC) addresses before allowing network access. A list of approved MAC addresses can be stored on the access point or on a remote server. These lists may be created and maintained manually or through an automated registration process. MAC addresses are relatively easy to change, however, so an intruder need only sniff the WLAN long enough to obtain a list of valid addresses and assume the identity of an inactive client to gain network access.
- **SSID (Server Set identifier)**
The SSID is a 32-byte string also known as the *network name*. With proper configuration, only clients with the correct SSID can communicate with the access point. In effect, the SSID acts as a single shared password between access points and clients. Access points come with default SSIDs. If not changed, these units are easily compromised. Furthermore SSIDs are often broadcast by access points and are easily detected by sniffing wireless packets. A *closed system* is one which does not respond to clients with the “Any” SSID assigned, nor does it broadcast the SSID to the clients at large.
- **WEP (Wired Equivalent Privacy protocol)**
The IEEE 802.11 standard also provides privacy between stations through an encryption scheme referred to as Wired Equivalent Privacy (WEP). Either 40-bit or 128-bit encryption keys must be shared between access points and wireless clients.

The three basic security services defined by IEEE for the WLAN environment are as follows:

- **Authentication** - A primary goal of WEP was to provide a security service to verify the identity of communicating client stations. This provides access control to the network by denying access to client stations that cannot authenticate properly.
- **Confidentiality** - Confidentiality, or privacy, was a second goal of WEP. It was developed to provide “privacy achieved by a wired network.” The intent was to prevent information compromise from casual eavesdropping (passive attack).
- **Integrity** - Another goal of WEP was a security service developed to ensure that messages are not modified in transit between the wireless clients and the access point in an active attack.

A WEP-encrypted message is constructed as follows:

The secret key is concatenated with an IV (Initialization Vector) and the resulting seed is input to the pseudorandom number generator (PRNG). The PRNG uses the RC4 stream cipher to output a key sequence of pseudorandom octets equal in length to the number of data octets that are to be transmitted.

In an attempt to protect against unauthorized data modification, an integrity check algorithm operates on the plaintext message to produce a checksum that is concatenated onto the plaintext message to produce the integrity check value (ICV). Encipherment is then accomplished by mathematically combining the ICV and PRNG output through a bit-wise XOR to generate the ciphertext. The IV is concatenated onto the ciphertext and the complete message is transmitted over the radio link. (Figure 3)

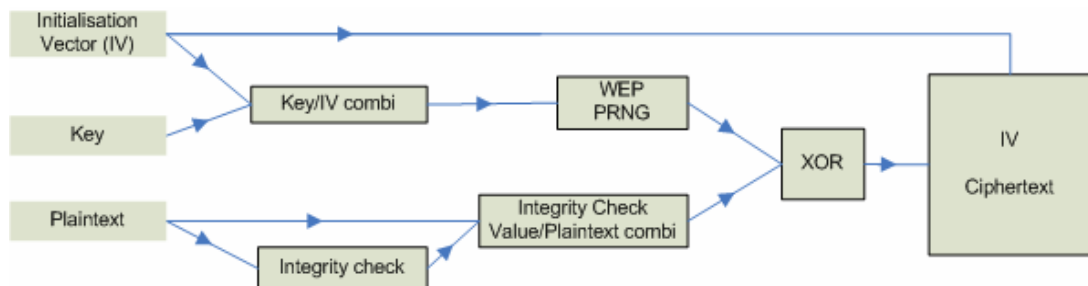


Figure 3: WEP encipherment

Shared key authentication can be summarized as follows: The access point sends the station a text challenge. The station encrypts the challenge using the shared key and returns the encrypted string to the access point. If the access point decrypts the response and recovers the original challenge, the authentication succeeds and the station is granted access. This represents unidirectional authentication; the wireless client is authenticated to the access point but not vice-versa. Furthermore, note that it is the wireless device and not the user that is being authenticated.

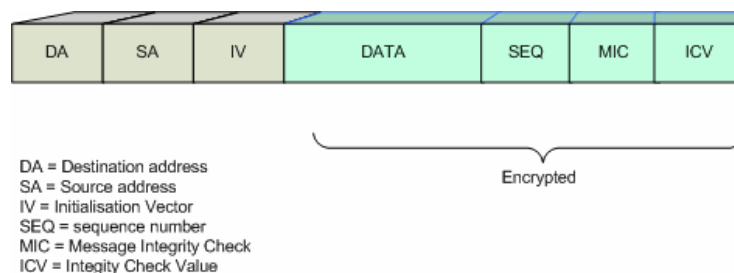


Figure 4: A WEP packet

WEP has been proven to be vulnerable to attack, as first documented by *Shamir, Mantin and Fluhrer* [WEP1] in August, 2001. In that paper, the authors provide mathematical and theoretical justification to claims that the RC4 stream cipher used by WEP uses a weak key scheduling algorithm.

AirSnort [AIRS] and WEPCrack [WEPC] are the two best known public tools for disclosing WEP keys.

- **Protocol Filters**

Protocol filters are set in place on routers and access devices that correspond to the edge of the network as far from the destination as possible. They are implemented in the form of a firewall rules set that follows the pattern of denying or permitting types of traffic based on port ID (like port 25) or well known protocol names such as the Simple Mail Transfer Protocol (SMTP). Filtering protocols is a relatively effective method of restricting WLAN users from attempting SNMP access to the wireless devices to alter configurations. In this way, the administrator can allow the administrative group access solely from the wired side of the LAN, or via console access. Another good policy with respect to protocol filtering on the WLAN is preventing the use of large Internet Control Message Protocol (ICMP) packets and other such protocols from being used as DoS-agents. You should also filter FTP from the WLAN if not otherwise required.

SNMP Monitoring

SNMP is a very powerful protocol for managing network-connected devices. Most access points have some manner of SNMP interface. Most access points are configured either via an SNMP interface or a web interface. Even the access points with a web interface have an SNMP system for remote monitoring. SNMP employs the concept of *managers* and *agents*. *Managers* are centralized hosts that make SNMP requests to devices that run agents. The *agents* then process the request and send response data back to the manager. Agents can also send traps. A problem with SNMP is that it is easily sniffed.

Cisco offers the *CiscoWorks Wireless LAN Solution Engine* for access point management. The description below came from the Cisco website.

The CiscoWorks WLSE is a centralized, systems-level solution for managing the entire Cisco Aironet WLAN infrastructure. The advanced radio frequency (RF) and device management features of the CiscoWorks WLSE simplify the everyday operation of WLANs, ensure smooth deployment, enhance security, and maximize network availability, while reducing deployment and operating expense. The CiscoWorks WLSE enables administrators to detect, locate, and mitigate rogue access points and RF interference. The assisted site survey feature automates the previously manual, expensive, and time consuming process of determining optimal access point settings including transmit power and channel selection. The CiscoWorks WLSE automatically configures access points and bridges, assures the consistent application of security policies, and proactively monitors faults and performance. The CiscoWorks WLSE is a core component of the Cisco Structured Wireless-Aware Network.

The authentication process

A wireless client that desires access to a WLAN must first undergo the authentication process. This authentication process validates information about the client's identity and is the initial step in connecting with the wireless access point. The authentication process may use two types of authentication:

- Open System Authentication
- Shared Key Authentication

With Open System Authentication (OSA) all negotiation is done in clear text and it will allow a client to associate to the access point without possessing the proper WEP key. The only thing that is needed is the proper SSID. An access point can be configured for OSA but still be configured for WEP data encryption. So if a client does properly associate to the access point, the client will be unable to encrypt or decrypt data it receives.

In contrast to OSA, Shared Key Authentication (SKA) forces the access point to send a challenge text packet to the wireless client. The client in turn, will encrypt the challenge text with its WEP key and send it back to the access point. The access point will then decrypt the challenge and compare it to the original text sent. If the two match, the access point will allow the client to associate with it.

The association process

The Association Process is the course of action in which a wireless client pursues a connection with an access point. The Association Process is the final step in connecting to a wireless access point.

The 802.11 standard indicates that the client must first authenticate to the access point and then associate to the access point. The standard also specifies that these two aforementioned processes will make up one of three states in the sequence joining a WLAN through an access point. The three states are:

- State 1: unauthenticated and unassociated
- State 2: authenticated and unassociated
- State 3: authenticated and associated

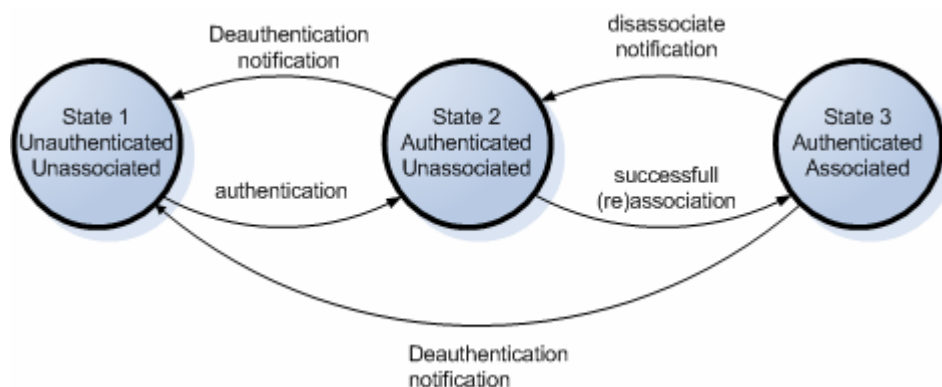


Figure 5: Client states

Unauthenticated and unassociated is the initial state of an access point and a client. Once a client has completed the authentication process but has yet to complete the association process, the client is considered to be in the second stage known as authenticated and unassociated. After the client successfully associates to an access point, the client has completed the final state and is considered to

be authenticated and associated. The client must be authenticated and associated with an access point before access to a WLAN is granted.

There are three phases in the development of a client becoming authenticated and associated to an access point. The three phases that make up this state are:

- Probing Phase
- Authentication Phase
- Association Phase

These phases are described in detail below:

Probing Phase

A wireless client will send a probe request packet out on all channels and any access point that is in range of the client will respond with a probe response packet. These access point probe response packets contain information that the client will use in the association process.

Authentication Phase

As stated earlier, the authentication phase can use either OSA or SKA. The configuration of the access point will dictate which type of authentication is used.

In the OSA scheme, a client will send an authentication request packet to the access point. The access point will analyze the authentication request packet and send an authentication response packet back to the client stating whether it is allowed to move onto the association phase.

In the SKA scheme, a client goes through the same process as with OSA but the access point sends a challenge text to the client. As stated earlier, the client will take this challenge and use its static WEP key to encrypt the text. Once the client sends it back to the access point, the access point will then decrypt the challenge with its static WEP key and compare it to the original text sent. The access point will allow the client to move on to the association phase if the text was properly decrypted but if the access point found the text to be contradictory, it will prevent the client from accessing the WLAN.

Association Phase

In the association phase, the client will send an association request packet to the access point. The access point will send an association response packet back to the client stating whether the client will be allowed to have access to the WLAN. The "Authenticated and Associated" state is the final negotiation step between an access point and a wireless client. If there are no other security mechanisms (RADIUS, EAP, or 802.1X) in place, access to the WLAN is granted.

2.2 Known attacks and tools

2.2.1 Different types of attacks

Most attacks fall into seven basic categories:

- Insertion attacks
- Interception and monitoring of wireless traffic
- Jamming
- Client-to-client attacks
- Encryption attacks
- Attacks based on misconfigurations
- Social Engineering

These attacks are described in detail below:

Insertion attacks

These attacks are based on deploying unauthorized devices or creating new WLANs.

- **Unauthorized Clients** – An attacker tries to connect a wireless client, typically a laptop or PDA, to an access point without authorization. Access points can be configured to require a password for client access. If no password is required, an intruder can connect to the internal network simply by enabling a wireless client to communicate with the access point.
- **Rogue Access Points** – An organization may not be aware that internal employees (or others) have deployed wireless activities on the corporate network. This lack of awareness could lead to the previously described attack, with unauthorized clients gaining access to corporate resources through a rogue access point. Organizations need to implement a policy to ensure secure configuration of access points, plus an ongoing process in which the network is scanned for the presence of unauthorized devices.

Interception and Monitoring of Wireless Traffic

As in wired networks, it is possible to intercept and monitor network traffic across a WLAN.

The attacker needs to be within range of an access point (approximately 300 feet for 802.11b, without the use of an external antenna) for this attack to work, whereas a wired attacker can be anywhere where there is a functioning network connection. The advantage for a wireless interception is that a wired attack requires the placement of a monitoring agent on a compromised system. All a wireless intruder needs is access to the network data stream.

There are two important considerations to keep in mind with the range of 802.11b access points. First, directional antennae can dramatically extend either the transmission or reception ranges of 802.11b devices. Therefore, the 300 foot maximum range attributed to 802.11b only applies to normal, as-designed installations. Enhanced equipment also enhances the risk. Second, access points transmit their signals in a circular pattern, which means that the 802.11b signal almost always extends beyond the physical boundaries of the work area it is intended to cover. This signal can be intercepted outside buildings, or through floors in buildings.

- **Wireless Packet Analysis** – A skilled attacker captures wireless traffic using techniques similar to those employed on wired networks. Many of these attacks focus on the first part of the connection session, where the data would typically include the username and password. An intruder can then masquerade as a legitimate user by using this captured information to hijack the user session and issue unauthorized commands.
- **Broadcast Monitoring** – If an access point is connected to a hub rather than a switch, any network traffic across that hub can be potentially broadcasted out over the wireless network.

Because the Ethernet hub broadcasts all data packets to all connected devices including the wireless access point, an attacker can monitor sensitive data going over wireless not even intended for any wireless clients.

Jamming

Denial of service (DoS) attacks are also easily applied to wireless networks, where legitimate traffic can not reach clients or the access point because illegitimate traffic overwhelms the frequencies. WLANs send information via radio waves on public frequencies, thus they are susceptible to inadvertent or deliberate interference from their traffic using the same radio band. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency. If the attacker can create enough RF (Radio Frequency) noise to reduce the signal-to-noise ratio to an unusable level, then the devices within range of the noise will be effectively taken offline. The devices will not be able to pick out the valid network signal from all of the random noise being generated and therefore will be unable to communicate. In addition, cordless phones, baby monitors and other devices that operate on the 2.4 GHz band can disrupt a wireless network using this frequency. Unfortunately, practical defenses against such an attack are limited, other than to avoid using 802.11 networks for critical components of the network infrastructure. Furthermore network monitor tools can be used to localize the problem area. Some DoS attacks are aimed specifically against wireless clients. These are described below.

Client-to-Client Attacks

Some attacks on wireless clients are aimed at the client directly, bypassing the access point. An attacker can also imitate an access point and intercept sensitive data from the connecting clients. The most common client-to-client attack techniques are described below.

- **File sharing and other TCP/IP service attacks** – Wireless clients running TCP/IP services such as a web server or file sharing are open to the same exploits and misconfigurations as any user on a wired network.
- **Denial of Service (DoS)** – A wireless device floods other wireless client with bogus packets, creating a denial of service attack. DoS attacks can target many different layers of the network.
 - **Application layer DoS attack (OSI layer 7)**
An application layer DoS is accomplished by sending large amounts of otherwise legitimate requests to a network-aware application, such as sending a large amount of page requests to a web server, swamping the server process. The goal of this type of attack is to prevent other users from accessing the service by forcing the server to fulfill an excessive number of transactions. The network itself may still be usable, but since the web server process cannot respond to the users, access to service is denied.
 - **Transport layer DoS attack (OSI layer 4)**
A transport layer DoS involves sending many connection requests to a host. This type of attack is typically targeted against the operating system of the victim's computer. A typical attack in this category is a SYN flood. All TCP connections begin with a three-way handshake, which starts with a packet having the SYN code bit set being transmitted by a client to a server. The server responds with a SYN-ACK packet based on the initial sequence number from the source. SYN flood attacks undermine this mechanism by sending a large number of SYN packets to the target system. When the target receives more SYN packets than it can handle, other legitimate traffic will not be able to reach the victim. One way to perform a SYN flood is to fill the connection queue of the target with half open connections. Once the target system receives the SYN packet and sends its SYN-ACK response, it will wait for the third part of the handshake. To make sure no RESET packets are returned, spoofed source addresses that are unresponsive on the Internet have to be used.
Most operating systems have a limit to the number of connections per second they will accept and a limit on the maximum number of connections they will maintain. A successful SYN flood will overwhelm the operating system on one of these two limits, thereby denying access to the services running on that host. As is the case in the

application-based DoS, the network is usually still functional, but the target host is unresponsive.

- **Network layer DoS attack (OSI layer 3)**

A network layer DoS is accomplished by sending a large amount of data to a network. This type of attack targets the network infrastructure of the victim. A typical network-based DoS attack is a ping flood. An attacker generates massive amounts of ICMP traffic destined for the victim network. (ICMP packets are used for management functions such as querying the availability and services of a host.) If a network allows any client to associate, it is vulnerable to a network-level DoS attack. Since an 802.11 network is a shared medium, a malicious user can flood the network with traffic, denying access to other devices associated to the affected access point.

- **Data-Link layer DoS attack (OSI layer 2)**

A data-link layer DoS can target either a host or a network. Data-link attacks are launched to disable the ability of hosts to access the local network even though the hosts are still connected. An example of this would be flooding a non-switched Ethernet network with invalid frames. An attacker (or sometimes a malfunctioning NIC) can send repeated frame headers with no payload. These headers are rebroadcast to all hosts on the network and effectively tie up the medium.

- **Physical layer DoS attack (OSI layer 1)**

This denial of service attack is described in the paragraph “Jamming” earlier.

Dos attacks based on Management frames

Management frames that control client-connection operations are complete unauthenticated meaning that anyone can change the MAC address of their NIC card and send frames that appear to come from another device. Essentially, an attacker can forge a packet so that it appears as if it originates at the access point to one or all the clients on the network. This packet tells these clients to disconnect. If this process is repeated enough times, stations will assume the WLAN is no longer available and will begin scanning for a new access point

A tool that is capable of this type of attack is included in the Air-Jack suite [AIRJ].

- **Malicious Association/ rogue access points** – Hackers can force wireless clients to an undesired 802.11 network or alter the configuration of the client to operate in ad-hoc mode. For this type of attack the hacker changes his laptop to operate as an access point. This ‘access point’ responds to the association request of the client and begins a connection. When connected, the hacker assigns an IP address to the client and begins his attacks. Note that the attacker can also be a college using a rogue access point attached to the network.

- **Access Point Clone Traffic Interception / Man-in-the-Middle” (MIM) attack** –

An attacker fools legitimate wireless clients into connecting to the attacker’s own network by placing an unauthorized access point with a stronger signal in close proximity to wireless clients (Figure 6). Since there is a one-way authentication the client will not notice connecting to a fake access point. Users attempt to log into the substitute servers and unknowingly give away passwords and similar sensitive data. EAP-TLS has a two-way-authentication method and can prevent such attacks.

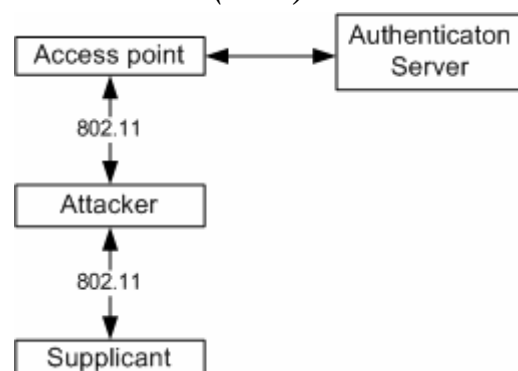


Figure 6: MitM attack

Session hijacking –is based on the lack of message confidentiality and low-layer authentication. The technique works as follows: an attacker can pose as the access point to the mobile station, and pose as the mobile station to the access point. First, it fakes a packet to the mobile station as if it came from the access point, telling the mobile station to “disassociate”, or drop its connection. Then, the attacker “hijacks” that connection, using the mobile station’s MAC-address to fool the access point into exchanging data with it. Figure 7 below shows three states in the connection to an access point.

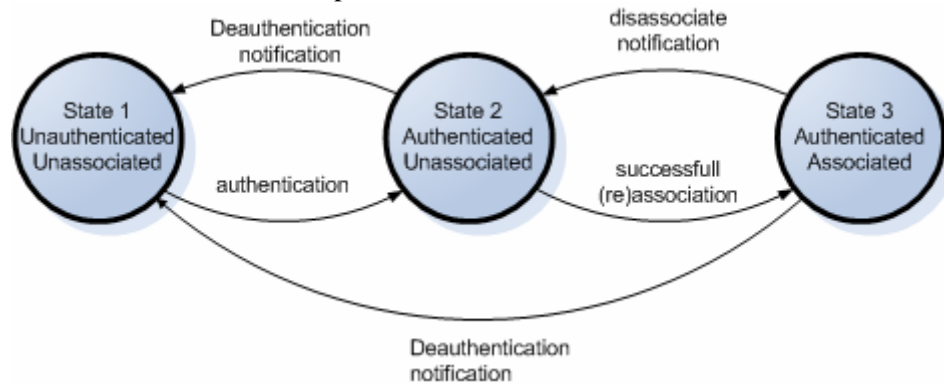


Figure 7: Setting up a connection

Figure 8 shows how an attacker could gain network access using session hijacking.

1. Messages 1, 2 and 3: A supplicant authenticates itself (Figure 8)
2. The attacker sends an 802.11 disassociate management frame using the access point’s MAC address. This causes the supplicant to get disassociated (message 4)
3. The attacker gains network access using the authenticated supplicants MAC address.

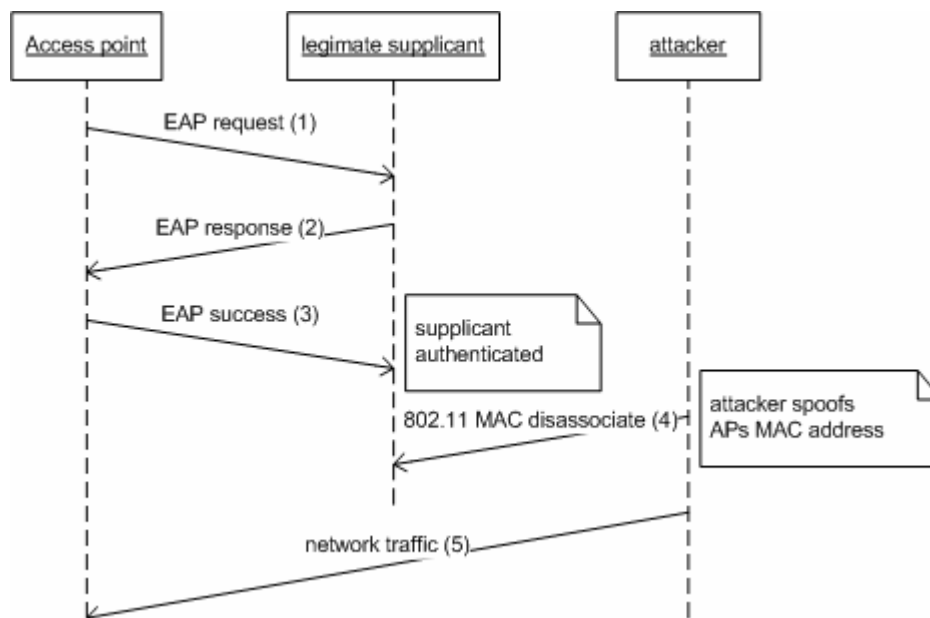


Figure 8: Session hijacking in detail

- **Address Resolution Protocol (ARP) cache poisoning** – Address resolution protocol cache poisoning is a MAC layer attack that can only be carried out when an attacker is connected to the same local network as the target machines. Most 802.11b access points act as transparent MAC layer bridges, which allow ARP packets to pass back and forth between the wired and wireless networks. This implementation choice for access points allows ARP cache poisoning attacks to be executed against systems that are located behind the access point. In unsafe deployments, wireless attackers can compromise traffic between machines on the wired network behind the wireless network, and also compromise traffic between other wireless machines including roaming clients in other cells.

A brief overview of various ARP based attacks and tools can be found in the paper: *An introduction to ARP spoofing* [PAC1]. The address resolution protocol serves the function of determining the mapping between IP addresses and MAC hardware addresses on local networks. For example, a host that wants to send a message to another host with IP-address 10.0.0.2 on the local network and sends a broadcast ARP packet that requests the MAC for that IP. The host that owns the IP 10.0.0.2 returns an ARP reply packet with its MAC address. The requesting host then sends the message, and stores the IP-to-MAC mapping for future packets.

This technique makes many types of *Man-in-the-Middle attacks* possible. One attack scenario is described below.

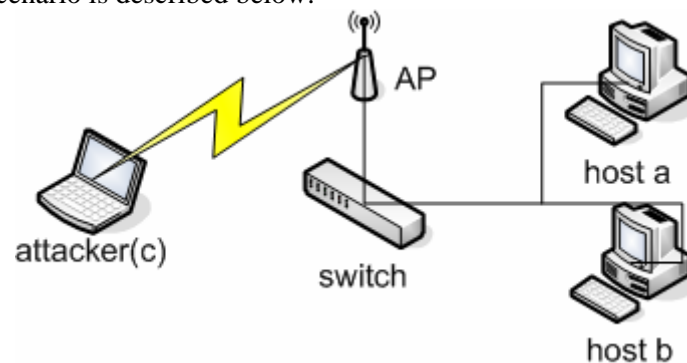


Figure 9: A MitM attack scenario

A wireless attacker can perform a *Man-in-the-Middle attack* against two machines on the wired network connected to the same switch as the access point (Figure 9).

The attacker (C) sends an ARP reply to host B stating that A's IP maps to C's MAC address, and another ARP reply to host A stating that B's IP maps to C's MAC address. Since ARP is a stateless protocol, hosts A and B assume they sent an ARP request at some point in the past and update their ARP caches with this new information. Now, when host A tries to send a packet to B it will go to C instead. Host C can use this unique position to forward the packets on to the correct host and monitor or modify them as they pass through C. This *Man-in-the-Middle attack* allows C to monitor or modify telnet sessions, read mail passing over POP or SMTP, intercept SSH negotiations, monitor and display Web usage, and commit many other activities. The same technique can be used to intercept or change the data stream between two wireless clients connecting through an access point (Figure 10). Ettercap [ETTE] is a tool for this type of attacks.

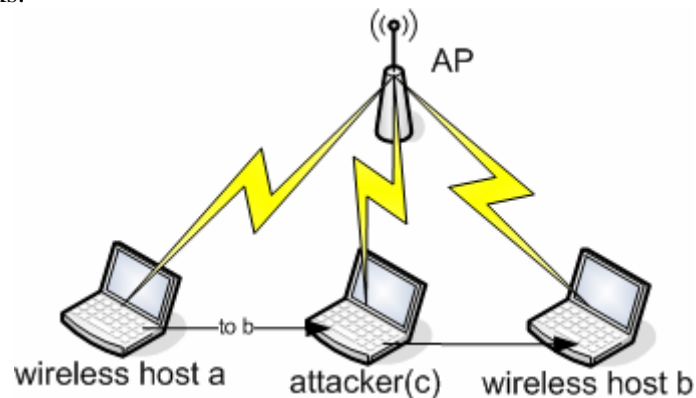


Figure 10: ARP attack against two wireless clients

Attacks against Encryption

- **FMS attacks** - 802.11b standard uses an encryption system called WEP (Wired Equivalent Privacy). As mentioned above WEP has been proven to be vulnerable to attack. The *FMS attack* (Fluhrer, Mantin, and Shamir) is based on three main principles:
 - Some IVs set up RC4 cipher the way it can reveal key information in its output bytes.
 - Invariance weakness allows use of the output bytes to determine the most probable key bytes.
 - The first output bytes are always predictable because they contain the SNAP header defined by the IEEE specification.

Detailed information on the FMS attack can be found in “*Weaknesses in the Key Scheduling Algorithm of RC4*” [WEP1] and “*Practical Exploitation of RC4 weaknesses in WEP environments*” [WEP2].

The disadvantage of FMS attacks is that one has to capture enough encrypted data to crack the key. In a high traffic network, this can be accomplished in a matter of hours. However, in a low traffic environment, this process can take days or weeks. Of course you can simply be patient and resort to doing sneaky things like putting *AirSnort* (or other tools) on a PDA and placing it in the bushes near the access point for days, but there are more clever techniques to artificially generate network traffic in order to capture more ciphertext to crack the key.

One possible packet injection attack works like this: The attacker will capture the encrypted traffic and look for a known protocol negotiation based on the size of the captured packet; for example, an ARP request has a predictable size (28 bytes). Once captured, the attacker can simply re-inject the encrypted packet (ARP request) over and over again. The ARP response will generate new traffic, which the attacker can then capture. If the attacker repeats this process, it is possible to generate enough traffic for a successful FMS attack in about an hour.

Figures 10 and 11 show how this attack might be carried out.

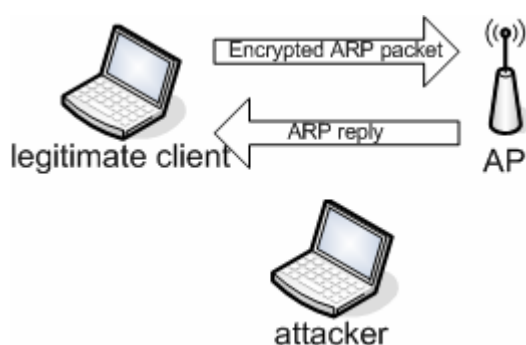
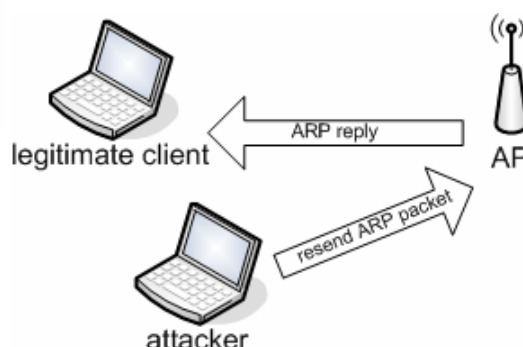


Figure 11: Capturing a packet

The attacker captures a legitimate, encrypted packet and guesses that it is an ARP request based on a known size (28 bytes).

Figure 12: Reinjecting the captured packet.

The attacker floods the network with the reinjected ARP reject. This results in a flood of ARP responses, which the attacker captures as part of an FMS attack.



Even more, the attacks on WLANs could include host discovery and even port scanning via the wireless traffic injection without even knowing WEP. TCP SYN's can be predictable and thus injected. The same applies to TCP ACK's, TCP RST's, TCP SYNACK's, and ICMP unreachable's such as ICMP port unreachable. At the moment, only one tool to launch attacks of this class, *Wepwedgie*[WEPW] is available.

Changing WEP keys on a regular basis would reduce the number of IV collisions, making it harder for those wishing to attack the wireless network. However, each time you change your key it is a manual process. Changing your encryption key in windows XP can be accomplished by changing the key under *my computer > control panel > network neighborhood > wireless connection > properties > tab wireless connections > network name > properties* (Figure 13)

As you can see, this process is quite involved and one might expect many people will rarely change the key they are using—especially home users, once they realize they will have to also define the key for their access point each time as well. In fact, many people who deploy wireless networks for both home and offices tend to just use the default WEP secret key. In many cases this key is standardized in such a way that attackers need only refer to their list of manufactures' defaults once they have identified which equipment you are using.

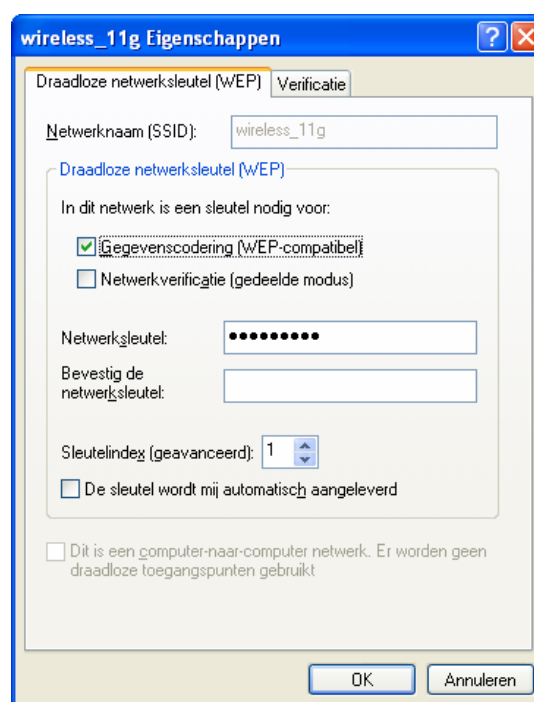


Figure 13: Network settings

Most vendors began implementing weak key avoidance in their firmware to protect against this attack. This weak key avoidance technique renders the FMS attack useless. The obvious answer to the *WEP* problem is to extend the *IV* space and don't reuse *IV*s. These issues (and others) are addressed in the *WPA* protocol

- **Brute force attacks** – In a brute force attack an attacker tries all possible combinations to find a password. Most MS-CHAP based authentication algorithms, such as Cisco LEAP are vulnerable to offline password attacks. During this attack a hacker captures the challenge-response messages exchanged between the client and the access point. Then the hacker tries to break the password with a dictionary or brute force attack.
The shared secret portion of the *WEP* key is either 40 bits or 104 bits, depending on which key strength you are using. Key generators from some vendors are flawed. A brute force attack on a 40-bit key using a weak key generator could take less than a minute to crack.
Key generators enable a user to enter a simple pass phrase to generate the key, instead of entering the key manually with hexadecimal numbers. A 40-bit *WEP* key shared secret would require 10 hexadecimal numbers; a 104-bit *WEP* key shared secret would require 26 hexadecimal numbers. As a convenience, some vendors allow you to enter a pass phrase in ASCII that will generate the 10 or 26 hexadecimal numbers for you. The use of a key generator is completely proprietary and not part of any standard. However, note that several different vendors all use the same key generation algorithm.
- **IV/WEP key replay** – The hacker send a plaintext to a client using the MAC address of the access point. The client sends the encrypted text back to the hacker. The hacker uses the response to derive the secret key.
- **Bit flipping** – Bit flipping works as follows:
 - The hacker intercepts a WEP-encrypted packet.
 - The hacker flips a bit in packet, recalculates ICV CRC32 and adds this to the message.
 - The hacker transmits the frame to the access point.
 - The access point forwards the frame (CRC32 is correct).
 - The layer 3 device rejects the frame and sends a predictable response to the access point.
 - The access point encrypts the response and sends it to the attacker.
 - The hacker uses the response to derive the secret key.

Misconfiguration

A company can buy the most expensive equipment, but if its administrator doesn't have the time or the knowledge to configure it in the right way, it will remain at a high risk for attack or misuse. This section describes the most common configuration flaws.

- **Server Set ID (SSID)** –Access points come with default SSIDs. Here are common default SSIDs and passwords:

Brand	Default SSID	Default username/password
Cisco	"tsunami"	Cisco/Cisco
3Com	"101"	-/comcomcom
Lucent/Cabletron	"RoamAbout Default Network Name"	-/
Compaq	"Compaq"	
Addtron	"WLAN"	
Intel	"intel"	-/Intel
Linksys	"linksys"	Admin/Admin
Other manufacturers	"Default SSID", "Wireless"	Admin/public/root/access
BreezeCOM	?	-/Super en -/laflaf

SSIDs go over the air as clear text if WEP is disabled, allowing the SSID to be captured by monitoring the network's traffic.

- **Wired Equivalent Privacy (WEP)** – WEP can be typically configured as follows:
 - No encryption
 - 40 bit encryption
 - 104 bit encryption

Most access point's ship with WEP turned off. Although 128 bit encryption is more effective than 40 bit encryption, both key strengths are subject to WEP's known flaws.

- **SNMP Community Passwords** – Many wireless access points run SNMP agents. If the community password is not properly configured, an intruder can read and potentially write sensitive data on the access point. If SNMP agents are enabled on the wireless clients, the same risk applies to them as well. By default, many access points are read accessible by using the community word, "public". 3Com access points allow write access by using the community word: "comcomcom". Cisco and Lucent/Cabletron require the write community word to be configured by the user or administrator before the agent is enabled.
- **Client Side Security Risk** – Clients connected to an access point store sensitive information for authenticating and communicating to the access point. This information can be compromised if the client is not properly configured. Cisco client software stores the SSID in the Windows registry, and the WEP key in the firmware, where it is more difficult to access. Lucent/Cabletron client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry, but it is encrypted using an undocumented algorithm. 3Com client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry without encryption.

Social engineering

As successfully used for wired systems, social engineering is a powerful technique for wireless systems as well. Most articles on social engineering give some sort of definition like "an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system". Social engineering is the 'art' of utilizing human behavior to breach security without the participant (or victim) even realizing that they have been manipulated or "getting needed information (for example, a password) from a person rather than breaking into a system". The only thing that everyone seems to agree upon is that social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him to gain unauthorized access to a valued system and the information that resides on that system.

There are two main categories under which all social engineering attempts could be classified: computer or technology based deception, and human based deception.

The technology-based approach is to deceive the user into believing that he is interacting with another computer system and get him to provide confidential information. For example, the user gets a pop-up window, informing him that the computer application has had a problem, and the user will need to reauthenticate in order to proceed. Once the user provides his ID and password on that pop up window, the harm is done. The hacker who has created the pop-up now has the user's ID and password and can access the network and the computer system.

The human approach is done through deception, by taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked. For example, the attacker impersonates a person with authority. He places a call to the help desk, and pretends to be a senior manager, and says that he has forgotten his password and needs to get it reset right away. The help desk person resets the password and gives the new password to the person waiting at the other end of the phone. At the very

least, the hacker can now access the personnel systems as if he were the manager, and obtain the social security numbers and other confidential/private information of several employees. He could of course do more damage to the network itself since he now has access to it.

Common techniques used in Social Engineering:

- ***Social Engineering by phone***

The most prevalent type of social engineering attack is conducted by phone. A hacker will call up and imitate someone in a position of authority or relevance and gradually pull information out of the user. Help desks are particularly prone to this type of attack. Hackers are able to pretend they are calling from inside the corporation by playing tricks on the PBX or the company operator, so caller-ID is not always the best defense.

Help desks are particularly vulnerable because they are in place specifically to *help*, a fact that may be exploited by people who are trying to gain illicit information. Help desk employees are trained to be friendly and give out information, so this is a gold mine for social engineering. Most help desk employees are minimally educated in the area of security and get paid peanuts, so they tend to just answer questions and go on to the next phone call. This can create a huge security hole.

- **Dumpster Diving**

Dumpster diving, also known as trashing is another popular method of social engineering. A huge amount of information can be collected through company dumpsters.

- Company phone books and organization charts provide phone numbers and locations of employees, especially management level employees who can be impersonated to the hacker's benefit.
- Memos provide small tidbits of useful information for creating authenticity.
- Procedure and policy manuals can help the hacker to become knowledgeable about the company's policies and procedures, and thus be able to convince the victim about their authenticity.
- Calendars are great. They may tell attackers which employees are out of town at a particular time.
- The hacker can use a sheet of paper with the Company letterhead to create official looking correspondence.
- Finally, outdated hardware, particularly hard drives, can be restored to provide all sorts of useful information. There are ways to retrieve information from disks, even if the user thinks the data has been 'deleted' from the disk.

- **Spying and eavesdropping**

A clever spy can determine the ID and password by observing a user typing it in. All he needs is to be there behind the user and be able to see his fingers.

If the policy is for the helpdesk to communicate the password to the user via the phone, then if the hacker can eavesdrop or listen in to the conversation, the password has been compromised. An infrequent computer user may even be in the habit of writing the ID and password down, thereby providing the spy with one more avenue to get the information.

- **Technical expert**

Take the case where the intruder posing as a support technician working on a network problem requests the user to let him access his workstation and 'fix' the problem. The unsuspecting user, especially if he is not technically savvy, will probably not even ask any questions, or watch while his computer is taken over by the so called technician. Here the user is trying to be helpful and doing his part in trying to fix a problem in the company's network.

- **On-Line Social Engineering**

The Internet is fertile ground for social engineers looking to harvest passwords. The primary weakness is that many users often repeat the use of one simple password on every account: Yahoo, University mail, EBay, whatever. So once the hacker has one password, he can probably get into multiple accounts. One way in which hackers have been known to obtain this kind of password is through an on-line form: they can send out some sort of sweepstakes information and ask the user to put in a name (including e-mail address – that way, she might even get that person's corporate account password as well) and password. These forms can be sent by e-mail or through Mail. Mail provides a better appearance that the sweepstakes might be a legitimate enterprise.

Furthermore, pop-up windows can be installed by hackers to look like part of the network and request that the user reenter his username and password to fix some sort of problem.

E-mail can also be used for more direct means of gaining access to a system. For instance, mail attachments sent from someone of authenticity can carry viruses, worms and Trojan horses.

- **Reverse Social Engineering**

A final, more advanced method of gaining illicit information is known as “reverse social engineering”. This is when the hacker creates a person that appears to be in a position of authority so that employees will ask him for information, rather than the other way around. If researched, planned and executed well, reverse social engineering attacks may offer the hacker an even better chance of obtaining valuable data from the employees. However, this requires a great deal of preparation, research, and pre-hacking to pull off.

According to [SE06], the three parts of reverse social engineering attacks are sabotage, advertising, and assisting. The hacker sabotages a network, causing a problem arise. That hacker then advertises that he is the appropriate contact to fix the problem. When he comes to fix the network problem, he requests certain bits of information from the employees and gets what he really came for.

2.2.2 Short description of useful security and attack tools

This part describes some of the widely used tools for breaking-in and testing the security of WLANs. Most of these tools are used for both purposes. Obviously the best way to examine the security of your network as an administrator is to test it with the same tools attackers use.

Airopeek NX (Commercial) [AIRO] – is a windows-based commercial sniffer specialized for wireless traffic. To use this tool you will need a NIC that supports monitor mode on Windows.

AirSnort [AIRS] - is by far the most popular and best-known Linux tool in the industry specifically used for wireless packet cracking.

Cain [CAIN] - has a lot of features including ARP poisoning, password cracking and detection of wireless networks.

Dsniff [DSNI] –is a collection of tools for network auditing and penetration testing. Dsniff, Filesnarf, Mailsnarf, Msgsnarf, Urlnarf, and Webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.). Arpspoof, Dnsspoof, and Macof facilitate the interception of network traffic normally unavailable to an attacker (e.g., due to layer-2 switching). Sshmitm and Webmitm implement active Man-in-the-Middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

Ethereal [ETHE] - is a UNIX- and Windows-based network monitoring tool. Although not specifically designed for 802.11 analyses, it does support capturing and decoding 802.11 packets with Libpcap. Since the windows-based version is unable to capture management frames I prefer the *nix-based version.

Ettercap [ETTE] - is a suite for Man-in-the-Middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols (even ciphered ones) and includes many features for network and host analysis.

Kismet [KISM] - is a Linux -based wireless sniffer that has war-driving functionality. It allows you to track wireless access points and their GPS locations like Netstumbler, but offers many other features as well. Kismet is a passive network-detection tool that will cycle through available wireless channels looking for 802.11 packets that indicate the presence of a WLAN, such as beacons and association requests. Kismet can also gather additional information about a network if it can, such as IP addressing and Cisco Discovery Protocol (CDP) names. Included with Kismet is a program called GPSMap, which generates a map of the Kismet results.

Languard Network Security Scanner (Commercial) [LNSS] - checks a network for all potential methods that a hacker might use to attack it. By analyzing the operating system and the applications running on your network, LANguard identifies possible security holes and provides information such as the service pack level of the machine, missing security patches, open shares, open ports, services/applications active on the computer, key registry entries, weak passwords, users and groups, and more.

MS network monitor [MSNM] - is another windows-based monitoring tool. This one can not show packets in real-time. You have to stop monitoring to view and analyze the packets.

Netstumbler [NETS] –is a Windows-based war-driving tool that will detect wireless networks and mark their relative position with a GPS. Netstumbler uses an 802.11 Probe Request sent to the broadcast destination address, which causes all access points in the area to issue an 802.11 Probe Response containing network configuration information, such as their SSID and WEP status. When hooked up to a GPS, Netstumbler will record a GPS coordinate for the highest signal strength found

for each access point. Using the network and GPS data, you can create maps with tools such as Stumbverter and Microsoft Mappoint.

Sniffer Pro (Commercial) [SNPR] - is a commercial sniffer that only runs on windows 2000. An advantage of this tool compared to Ethereal is that this tool has expert analysis and can make a graphical representation of the traffic flow. On the other hand, Ethereal has a 'Follow TCP stream' option which I find very useful.

TCPdump [TCPD] - is a standard UNIX network monitoring tool that supports decoding 802.11 frame information in newer versions.

WEPCrack [WEPC] - is an open source tool for breaking 802.11 WEP secret keys.

WepLab [WEPL] - uses a full weak keys attack (FMS) to both first and second bytes for 64 bits or 128 bits keys (these optimizations are not present in Aircrack and WEPCrack)

AirCrack [AIRC] - is an 802.11 WEP key cracker. Aircrack is much more efficient as Aircrack. Aircrack usually requires more than five million unique IVs to crack a 104-bit WEP key, whereas Aircrack only needs many times less IVs. Additionally, post-2002 WiFi equipments filter the "interesting" IVs Aircrack relies on; on the other hand, Aircrack can break a WEP key without the need for said IVs.

Mac Makeup [MAMA], Smac[SMAC], Kmac[KMAC] and Etherchange [ETCH] - are MAC address changers for windows.

Airjack [AIRJ] - is a packet injection tool for *nix.

WEPWedgie [WEPW] - is a toolkit for determining 802.11 WEP keystreams and injecting traffic with known keystreams. The toolkit also includes logic for firewall rule mapping, pingscanning, and portscanning via the injection channel and a cellular modem.

LinkFerret Off-Line WEP Decrypter (Commercial) [LINK] - is a specialized tool, used to process and decrypt WEP'd data frames stored in an 802.11 trace file.

2.3 Advanced wireless security techniques

2.3.1 VPN

Basically, a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. There are two common types of VPN: Remote-access and site-to-site.

Remote-Access VPN

Remote-access, (e.g. a *virtual private dial-up network (VPDN)*), is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations. Typically, a corporation that wishes to set up a large remote-access VPN will outsource to an *Enterprise Service Provider (ESP)*. The ESP sets up a *network access server (NAS)* and provides the remote users with desktop client software for their computers. The telecommuters can then dial a toll-free number to reach the NAS and use their VPN client software to access the corporate network. Remote-access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.

Site-to-Site VPN

Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network such as the Internet. Site-to-site VPNs can be one of two types:

- **Intranet-based** - If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.
- **Extranet-based** - When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

VPN Security

A well-designed VPN uses several methods for keeping your connection and data secure:

- **Firewalls**
- **Encryption**
- **IPSec**
- **AAA Server**

These methods are described in detail below:

Firewalls

A firewall provides a strong barrier between the private network and the Internet. Some VPN products, such as Cisco's 1700 routers, can be upgraded to include firewall capabilities by running the appropriate Cisco IOS on them.

Encryption

Most computer encryption systems belong in one of two categories:

- Symmetric-key encryption
- Public-key encryption

In **symmetric-key encryption**, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one. The code provides the key to decoding the message.

Public-key encryption uses a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it.

Internet Protocol Security Protocol (IPSec) provides enhanced security features such as better encryption algorithms and more comprehensive authentication.

IPSec

IPSec has two encryption modes: tunnel and transport. Tunnel encrypts the header and the payload of each packet while transport only encrypts the payload. Only systems that are IPSec compliant can take advantage of this protocol. Also, all devices must use a common key and the firewalls of each network must have very similar security policies set up.

AAA servers

AAA (authentication, authorization and accounting) servers are used for more secure access in a remote-access VPN environment. When a request to establish a session comes in from a dial-up client, the request is proxied to the AAA server. AAA then checks, who you are (authentication), what you are allowed to do (authorization) and what you actually do (accounting)

The accounting information is especially useful for tracking client use for security auditing, billing or reporting purposes.

Tunneling

Most VPNs rely on **tunneling** to create a private network that reaches across the Internet. Essentially, tunneling is the process of placing an entire packet within another packet and sending it over a network. The protocol of the outer packet is understood by the network and both points, called **tunnel interfaces**, where the packet enters and exits the network.

Tunneling requires three different protocols:

- **Carrier protocol** - The protocol used by the network that the information is traveling over
- **Encapsulating protocol** - The protocol (GRE, IPSec, L2F, PPTP, L2TP) that is wrapped around the original data
- **Passenger protocol** - The original data (IPX, NetBeui, IP) being carried

Tunneling has amazing implications for VPNs. For example, you can place a packet that uses a protocol not supported on the Internet (such as NetBeui) inside an IP packet and send it safely over the Internet. Or you could put a packet that uses a private (non-routable) IP address inside a packet that uses a globally unique IP address to extend a private network over the Internet.

The identity of both the client and the authentication server is verified so that one is not vulnerable to Man-in-the-Middle attacks. The wireless access points can be configured for easy association.

Many VPNs have the option of *Split Tunnelling*. This means that the client can use both its assigned VPN address and its locally assigned IP address for network traffic. The organization might have secured the VPN address well but has seldom control of the client's local address. A hacker could attack the user's computer on the local address and then use the victim computer to gain access to the VPN secured network through the tunnel. Seen from the perspective where VPN is used for securing wireless networks, the hacker could use the inside address space to find a victim to hack and then use his tunnel as a bridge through the VPN concentrator. The VPN concentrator should be configured to disable *Split Tunnelling* and only allow traffic to pass through the VPN tunnel once established. Some VPN clients offer a personal firewall. One can also install a third party personal firewall. This could be a great way to enhance security but in either case the security is depending on the user's ability to correctly configure and use these firewalls.

Roaming between access points can cause problems and may require user interaction. Clients that are in the middle between two cells may have continues disconnection problems.

2.3.2 WEB based access and hotspot security

Web based access control is often used for commercial access points also known as hotspots. Generally the client needs a card with a login code that grants access to the Internet for a limited period of time. When the client connects to the access point he is redirected to a login screen. After verifying the login code access to the Internet is granted (or denied).

The most common hotspot providers in the Netherlands are enumerated below:

- Swisscom
- KPN
- Mobilander
- T-Mobile
- Vodafone
- WinQ
- Viawia
- Prorail

While many of the recommendations made for safeguarding a home or business network, WiFi hotspots present a whole new set of security issues, notably unknown computers sharing the same local network with you. Most (if not all) of the available hotspots today lack WEP or WPA encryption.

A search on the website of the providers above doesn't deliver any confirmation about the possible use of encryption, so I assume that all the hotspots in the Netherlands don't use encryption. This assumption is confirmed by *wirelessnederland.nl* who stated that 100% of the hotspots aren't using WEP or other form of security on their website. Their assumption is based on hundreds of wardrive sessions through the country.

The statement below is derived from the KPN website and concerns the security of the KPN hotspots:

Q: Welke gegevens worden "versleuteld"?

A: Alle gegevens die nodig zijn voor het inloggen en eventueel online betalen van toegang via een creditcard betaling, worden via "versleuteling" beschermd. Hieronder vallen uw inlogcode en wachtwoord, de online-tijd en de verzonden data. De interen vastgelegd. Uw anonimiteit blijft dan ook voor de duur van de internettoegang via Hotspots van KPN gewaarborgd. Hotspots van KPN stelt de gegevens niet beschikbaar aan derde partijen.

From this statement I conclude that only the authentication data is encrypted. Other data like email and web traffic are not encrypted by the hotspot provider.

T-Mobile says their hotspots are "*Fast, secure and easy to use*". However when I downloaded and read the manual [HS10] for hotspot usage, I discovered there isn't any encryption used at this providers hotspots either.

Highlight the 'Wireless Networks' tab. The network SSID tmobile should be visible under the 'Available networks' section. Ensure that the 'Data encryption (WEP enabled)' option is not selected, as T-Mobile Hotspot is a public service.

In the US *Boingo Wireless* is the first hotspot provider that has added 802.1x and WPA security support to its network of hotspots. Specifically, the hotspot vendor said it has released new end user client software that incorporates support for 802.1x and WPA security measures. Likely, providers in the Netherlands will add this support in the near future.

The lack of encryption doesn't imply you can't use hotspots. Below are some suggestions for a client to do to protect him while using a hotspot.

- ***Make sure you're connected to a legitimate access point!*** - Rogue access points in public areas will have the same SSID as what you'd expect (such as KPN or T-mobile), but really connect directly to hijackers' databases to collect the passwords and usernames you use to sign in. Even worse, they can collect credit card data from people who sign up for new accounts.
- ***Encrypt sensitive data*** - As you beam emails from your laptop to the wireless access point and back, or as you enter your username and password to check your bank account balances someone nearby can be intercepting those packets of data as they fly by. While data sent to and from secure web sites (those starting with https:) is generally protected, you can also use encryption in other contexts. If you are sending a sensitive file via email, for example, encrypt it first with a password.
- ***Use a Virtual Private Network*** - One of the best ways to protect your data when using a public wireless network or hotspot is to use a virtual private network (VPN). A VPN establishes a private network across the public network by creating a tunnel between the two endpoints so that nobody in between can intercept the data. Many companies allow remote users to connect to corporate networks as long as they use VPN. This keeps the users' communications just as secure as if they were sitting at a desk in the building. More details about a VPN can be found in paragraph 2.3.1.
- ***Use a Personal Firewall*** - When you connect to a public wireless network you are joining a local network with other unknown computers. Having these computers on the same IP subnet makes them more dangerous than machines elsewhere on the Internet. Machines in your network and subnet range are able to more easily capture traffic between your computer and the wireless access point or attempt to connect with your computer and access your files and folders.
- ***Use up-to-date anti-virus software*** - When you connect to a public network there's a real change other user of the same network are unintentionally or deliberately trying to infect you with a virus.
- ***Keep your OS and applications up to date*** - It seems that almost every week there's a new "security patch" for various parts of the Windows operating system or Office programs.
- ***Be aware of people around you*** - When you're at an ATM, you make sure no one can see you type your PIN. Be just as careful about typing in your name and password at a hotspot.
- ***Use a Web-based email program*** - when you're connecting at a public hotspot, instead of Outlook, Eudora, or Apple Mail. Most ISPs these days let you send and receive email via a Web interface as well as downloading it into your email program. These websites generally use secure sockets layer (SSL) or other security protocols, which protect your data while it's being transmitted.
- ***Make sure file sharing is off!***
- ***Use strong passwords for sensitive files and folders*** - as well as for access to your computer as a whole. Consider keeping your most important data on an encrypted USB keychain storage device.

Hotspots and Bluetooth

A security flaw in some implementations of Bluetooth enables hackers to easily steal WiFi hotspot authentication information. The Bluetooth flaw is exploited when users sign up for hotspot access using SMS text messaging (even the SMS requesting the hotspot account information can be sent by the attacker), a method allowed by a variety of hotspot providers. The Bluetooth security flaw enables nearby hackers to intercept the SMS message containing log-on information as it travels between the user and the hotspot vendor. In case the attacker sends the initiating message, any trace of malicious use can be removed by deleting the SMS from the mobile phone's memory. Measurements have shown that this attack will take an average of 30 - 45 seconds if the attack is automated by a script.

Additional suggestions for access including Bluetooth

- ***Check to see if your phone is vulnerable [BT4]*** - On this webpage phones are listed that are vulnerable to the "CHAOS" attack
- ***Check for firmware updates for your phone*** - Updates contain fixes for known vulnerabilities. Apply these updates to mitigate these vulnerabilities.
- ***Switch off Bluetooth visible mode*** - obviously undetected phones are less likely to be hacked.
- ***Don't use Bluetooth in public places*** - This reduces the chance of attacks as well as the power consumption of your phone.

2.3.3 The IEEE 802.1x standard

The IEEE 802.1x standard describes a way arrange access to a wired or WLAN independent of the authentication method. 802.1x supports the division of traffic flows of virtual networks. (For example students, guests and employees of a university can use the same access points to surf on the Internet but access to the production network is limited to the employees).

802.1x does solve the following security problems:

- Collecting and cracking of keys is very difficult, because every Client has its own key and the keys change over time.
- Man-in-the-Middle attacks using rogue access points (if both client and access point are authenticated)
- Unauthorized access by authenticating users and computers

802.1x does not solve the following problems:

- Bit flipping with known IVs -> sending false packets (keyed MIC is not supported).
- DOS attacks using disassociate messages

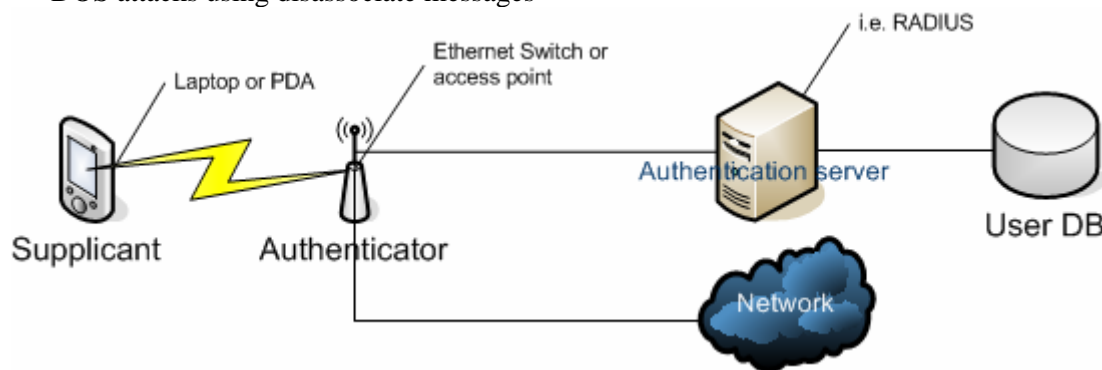


Figure 14: 802.1x elements

802.1x consists of the following parts:

- **Authenticator** - Generally this is a device such as an Ethernet switch to which another device seeking network access attaches via a point-to-point connection. In WLANs, the authenticator is an access point. Note that WLANs better represent shared media topologies than point-to-point configurations for which 802.1x was designed.
- **Authentication server** - As the name suggests, this is the actual source of authentication services provided to end points. This is one of the strengths of 802.1X, as it permits centralization of this service instead of requiring separate authentication services to run locally on each authenticator (although the standard does allow an entity to be both). Centralization simplifies the task of keeping the user credentials current and allows for server redundancy. Except in the smallest implementations, the authentication server would be expected to be a separate entity. When the authenticator and authentication server are separate, network connectivity between the two is assumed. In that case, the authenticator simply passes traffic between the supplicant (see definition below) and the authentication server.
- **Network access port** - This is a device's point of attachment to the network. Since wireless clients do not have physical network connections, an association between a wireless client and an access point is considered a network access port.
- **Supplicant / peer** - The supplicant is the entity on the opposite end of the point-to-point link from the authenticator. A wireless client is an example of a supplicant.

- **Extensible Authentication Protocol (EAP)** - EAP is “extensible” in the sense that any higher level authentication mechanism, such as one-time passwords, Kerberos, or some future technology may be used to validate the user’s login credentials. The authenticator is not required to have knowledge of these authentication protocols, and can serve as a simple pass-through device between the peer and authentication server. Once a “success” or “failure” message is sent to the peer the authentication phase is complete.
- **EAP over LAN (EAPOL)** - EAP over LAN describes how EAP packets are to be encapsulated within Ethernet, Token Ring or FDDI frames. This provides a communications path between the supplicant PAE and authenticator PAE over which authentication can take place. When EAP packets between the authenticator and the authentication server go across the network, they are encapsulated within a secure protocol such as RADIUS. Figure 15 below shows the encapsulation of packets during the authentication.

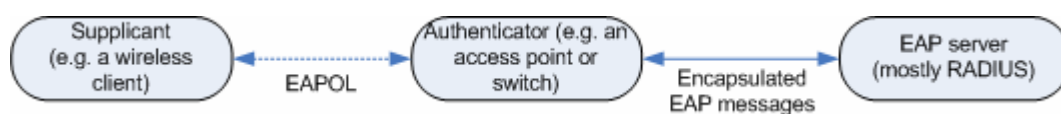


Figure 15: EAP over LAN

The access point must permit the EAP traffic before the authentication succeeds. In order to accommodate this two ports are used, a ‘controlled’ and ‘uncontrolled’ port. The uncontrolled port filters all traffic and allows only EAP packets to pass. The controlled port demands authentication of the client.

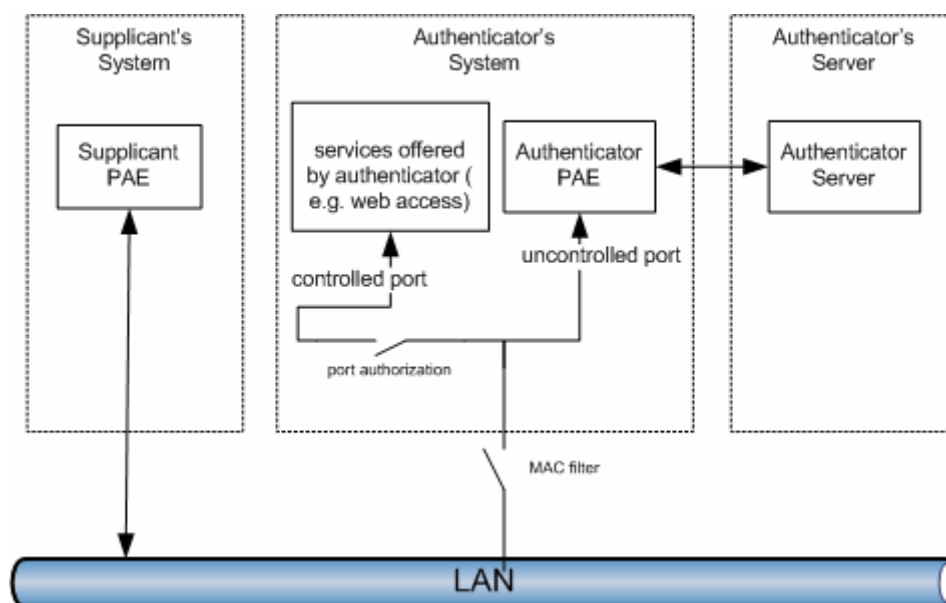


Figure 16: Entities in EAP authentication

Initial 802.1x communications begin with an unauthenticated supplicant (e.g., a client device) attempting to connect with an authenticator (e.g., an 802.11 access point). The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS). Once authenticated, the access point opens the client's port for other types of traffic.

An EAP-TTLS negotiation comprises two phases: the TLS handshake phase and the TLS tunnel phase.

Phase 1: Handshake

In phase 1 the TLS handshake protocol is used to authenticate the TTLS server to the client and, optionally, to authenticate the client to the TTLS server.

Phase 1 is initiated when the client sends an EAP-start message. This begins a series of message exchanges to authenticate the client. The access point replies with an EAP-request identity message. Now the client sends an EAP-Response/Identity packet to the authentication server. The authentication server responds to the EAP-Response/Identity packet with an EAP-TTLS/Start packet, which is an EAP-Request with Type = EAP-TTLS. This indicates to the client that it should begin TLS handshake by sending a ClientHello message.

EAP packets continue to be exchanged between client and authentication server to complete the TLS handshake. Phase 1 is completed when the client and authentication server exchange ChangeCipherSpec and Finished messages. At this point, additional information may be securely tunneled. As part of the TLS handshake protocol, the authentication server will send its certificate along with a chain of certificates leading to the certificate of a trusted CA. The client will need to be configured with the certificate of the trusted CA in order to perform the authentication.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_e2:45:16	00:77:77:77:77:77	EAP	Request, Identity [RFC3748]
2	0.013081	00:77:77:77:77:77	Cisco_e2:45:16	EAPOL	Start
3	0.014509	Cisco_e2:45:16	00:77:77:77:77:77	EAP	Request, Identity [RFC3748]
4	0.021837	00:77:77:77:77:77	Cisco_e2:45:16	EAP	Response, Identity [RFC3748]
5	0.051148	Cisco_e2:45:16	00:77:77:77:77:77	EAP	Request, EAP-TTLS [Funk]
6	0.074346	00:77:77:77:77:77	Cisco_e2:45:16	TLS	Client Hello
7	0.111263	Cisco_e2:45:16	00:77:77:77:77:77	EAP	Request, EAP-TTLS [Funk]
8	0.117191	00:77:77:77:77:77	Cisco_e2:45:16	EAP	Response, EAP-TTLS [Funk]
9	0.151237	Cisco_e2:45:16	00:77:77:77:77:77	EAP	Request, EAP-TTLS [Funk]
10	0.151969	00:77:77:77:77:77	Cisco_e2:45:16	EAP	Response, EAP-TTLS [Funk]
11	0.186092	Cisco_e2:45:16	00:77:77:77:77:77	EAP	Request, EAP-TTLS [Funk]
12	0.186816	00:77:77:77:77:77	Cisco_e2:45:16	EAP	Response, EAP-TTLS [Funk]
13	0.218781	Cisco_e2:45:16	00:77:77:77:77:77	TLS	Server Hello, Certificate, Certificate Request, Server Hello Done
14	0.401468	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xa8694e41
15	0.549881	00:77:77:77:77:77	Cisco_e2:45:16	TLS	Certificate, Client key Exchange, Change Cipher Spec, Encrypted H
16	0.587447	Cisco_e2:45:16	00:77:77:77:77:77	TLS	Change Cipher Spec, Encrypted Handshake Message
17	0.588327	00:77:77:77:77:77	Cisco_e2:45:16	TLS	Application Data
18	0.648438	Cisco_e2:45:16	00:77:77:77:77:77	EAP	Success
19	0.648818	Cisco_e2:45:16	00:77:77:77:77:77	EAPOL	Key
20	0.649258	Cisco_e2:45:16	00:77:77:77:77:77	EAPOL	Key
21	0.665676	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x217b6322

Figure 17: Authentication messages between client and authenticator

Phase 2: Tunnel

In phase 2 the TLS Record Layer is used to securely tunnel information between client and TTLS server.

Any type of information may be exchanged during phase 2, according to the requirements of the system.

This process continues until the TTLS server has enough information to issue either an EAP-Success or EAP-Failure. Thus, if the AAA server rejects the client based on forwarded authentication information, the TTLS server would issue an EAP-Failure. If the AAA server accepts the client, the TTLS server would issue an EAP-Success.

If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

Summarized the following are specific interactions that take place among the various 802.1x elements (Figure 18).

1. The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.
3. The client sends an EAP-response packet containing the identity to the authentication server.
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or other EAP authentication type.
5. The authentication server will either send an *accept* or *reject* message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

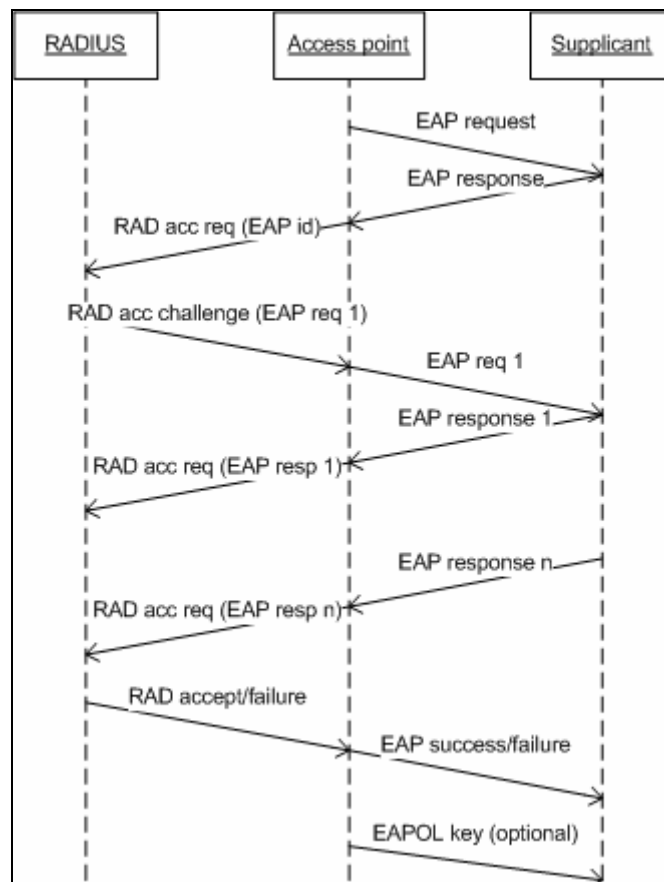


Figure 18: Authentication of a client

The traffic between the access point and RADIUS server is sent over the RADIUS protocol. Each access point has its own key.

EAP

An EAP packet contains five fields (Figure 19). The Code field, the first field in the packet, is one byte long and identifies the type of EAP packet. It is used to interpret the Data field of the packet and can accept four values (request, response, accept or failure). The Identifier field contains an unsigned integer used to match requests with responses to them. Retransmissions reuse the same identifier numbers, but new transmissions use new identifier numbers. The Length field is two bytes long. It is the number of bytes in the entire packet, which includes the Code, Identifier, Length, and Data fields. The last field is the variable-length Data field. Depending on the type of packet, the Data field may be zero bytes long.

Note that the data field can contain type information. This additional type field is used in *EAP request and response packets*. The Type field is a one-byte field that indicates the type of request or response. Only one type is used in each packet. With one exception, the Type field of the response matches the corresponding request. That exception is that when a request is unacceptable, the peer may send a NAK to suggest an alternative type. Types greater than or equal to four indicate authentication methods.

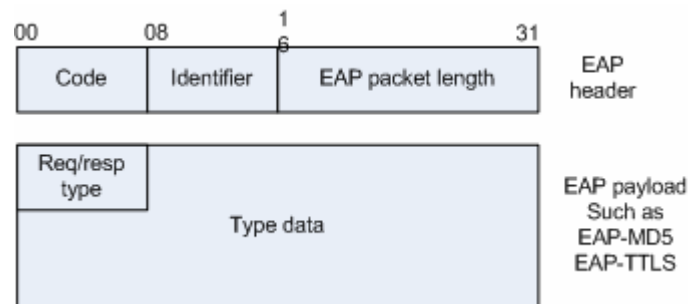


Figure 19: An EAP packet

The Type-Data field is a variable field that must be interpreted according to the rules for each type.

- Type code 1: Identity-** The authenticator generally uses the Identity type as the initial request. After all, identifying the user is the first step in authentication. Naturally, most implementations of EAP prompt the user for input to determine the user identity. The Type-Data field may contain text used to prompt the user. The length of the string is computed from the length field in the EAP packet itself.
- Type Code 2: Notification-** The authenticator can use the Notification type to send a message to the user. The user's system can then display the message for the user's benefit. Notification messages are used to provide messages to the user from the authentication system, such as a password about to expire. Responses must be sent in reply to Notification requests. However, they serve as simple acknowledgments, and the Type-Data field has a zero length.
- Type code 3: NAK -** NAKs are used to suggest a new authentication method. The authenticator issues a challenge, encoded by a type code. If the end user system does not support the authentication type of the challenge, it can issue a NAK. The Type-Data field of a NAK message includes a single byte corresponding to the suggested authentication type.
- Type code 4: MD-5 Challenge -** The MD-5 Challenge is used to implement the EAP analog of the CHAP protocol. Requests contain a challenge to the end user. For successful authentication, CHAP requires that the challenge be successfully encoded with a shared secret. All EAP implementations must support the MD-5 Challenge, but they are free to NAK it in favor of another authentication method.

- **Type code 5: One-time password (OTP)** - The Request issued to the user contains the OTP challenge string. Like all authentication types, responses may be NAKs.
- **Type code 6: Generic Token Card** - Token cards such as RSA's SecurID and Secure Computing's Safeword are popular with many institutions because they offer the security of "random" one-time passwords without the hassle of an OTP rollout. The Request contains the Generic Token Card information necessary for authentication. In the Response, the Type-Data field is used to carry the information copied from the token card by the user.
- **Type code 13: TLS** - When EAP is used over TLS is the standardized successor to the widely deployed Secure Socket Layer (SSL), and TLS authentication inherits a number of useful characteristics from SSL. Most notably, mutual authentication is possible with TLS.

Different types of EAP have been defined to support authentication methods and associated network security policies. The most widely-deployed EAP types are:

- **EAP-MD5** - lets a RADIUS server authenticate LAN stations by verifying an MD5 hash of each user's password. This is a simple and reasonable choice for trusted Ethernets where there is low risk of outsider sniffing or active attack. However, EAP-MD5 is not suitable for public Ethernets or WLANs because outsiders can easily sniff station identities and password hashes, or masquerade as access points to trick stations into authenticating with them instead of the real access point.
- **EAP with Transport Layer Security (EAP-TLS)** - is the only standard secure option for WLANs at this time. EAP-TLS requires the station and RADIUS server to both prove their identities via public key cryptography (e.g. digital certificates or smart cards). This exchange is secured by an encrypted TLS tunnel, making EAP-TLS very resistant to dictionary or other MitM attacks. However, the station's identity -- the name bound to the certificate -- can still be sniffed by outsiders. EAP-TLS is most attractive to large enterprises that use only Windows XP/2000/2003 with deployed certificates.
- **Cisco's Lightweight EAP (LEAP)** - goes a notch beyond EAP-MD5 by requiring mutual authentication and delivering keys used for WLAN encryption. Mutual authentication reduces the risk of access point masquerading -- a type of Man-in-the-Middle attack. However, station identities and passwords remain vulnerable to attackers armed with sniffers and dictionary attack tools. LEAP is mostly attractive to organizations that use Cisco access points and cards and want to modestly raise the security bar.
- **EAP with Tunneled TLS (EAP-TTLS) and Protected EAP (PEAP)** - are Internet Drafts that have been proposed to simplify 802.1x deployment. Both require certificate-based RADIUS server authentication, but support an extensible set of user authentication methods. Organizations that have not yet issued certificates to every station and don't want to just for 802.1x can use Windows logins and passwords instead. RADIUS servers that support EAP-TTLS and PEAP can check LAN access requests with Windows Domain Controllers, Active Directories, and other existing user databases. From a sniffing perspective, these options are just as strong as EAP-TLS. However, user passwords are still more likely to be guessed, shared, or disclosed through social engineering than client-side certificates.

Some authentication methods for TTLS are: PAP, CHAP and MS-CHAPv2

2.4 Legal provisions and requirements

‘Wet bescherming persoonsgegevens (WBP)’

This law concerns the obligation to protect private data. As an example, you have to keep your PIN secret to be able to lay any claim on compensation in case your card is stolen and used to withdraw your money.

Penal laws

1. Computer crime I (1993): This law concerns “computervredebreuk”. An attacker is only punishable if there is a certain level of security. As a result, using someone’s unprotected access point to access the Internet is not prohibited!
2. Computer crime II: This law contains some major adjustments to the first law, concerning email protection and (cracking of) encryption

Most important clauses concerning computer crime

The clauses below concern computer crime and activities alike

Article 138a lid1 WvSr: This clause concerns gaining unauthorized access to an automated network.

Article 138a lid1 sub a WvSr: This clause concerns gaining unauthorized access to an automated network by means of breaking any security.

Article 138a lid1 sub b WvSr: This clause concerns gaining unauthorized access to an automated network by means of the usage of a false key or identity.

Article 138a lid2 WvSr: This clause concerns unauthorized capturing stored information in a compromised automated network.

Article 139c lid1 WvSr: This clause concerns eavesdropping or the unauthorized recording of data.

Article 139c lid1 WvSr: This clause concerns the unauthorized installation of monitoring equipment.

Article 161sexties WvSr: This clause concerns deliberately causing disorder in an automated network (for instance jamming).

Article 350a lid1 WvSr: This clause concerns deliberately destroying or changing data.

Table 1: Legal provisions concerning computer crime

2.5 The Utwente WLAN

In this paragraph I summarize public available information about the security measures implemented to protect the WLAN. These measures can be divided into three categories

- Management measures, these include things such as user agreements and policy;
- Operational measures, these include physical security of the access points;
- Technical measures, these include things such as authentication and firewalls.

VLAN division according to WLAN@UT:

Cisco access points provide the possibility to assign different SSIDs to the BSSID

VLAN	Name	Comment
1	WLAN	The AP's are in this network
2	WLANATUT	VLAN for employees and students
3	GUEST	VLAN for guest use
4	COM1	VLAN for commercial use / test
5	COM2	idem
6	COM3	idem
7	COM4	idem
8	COM5	idem

Table 2: WLAN division

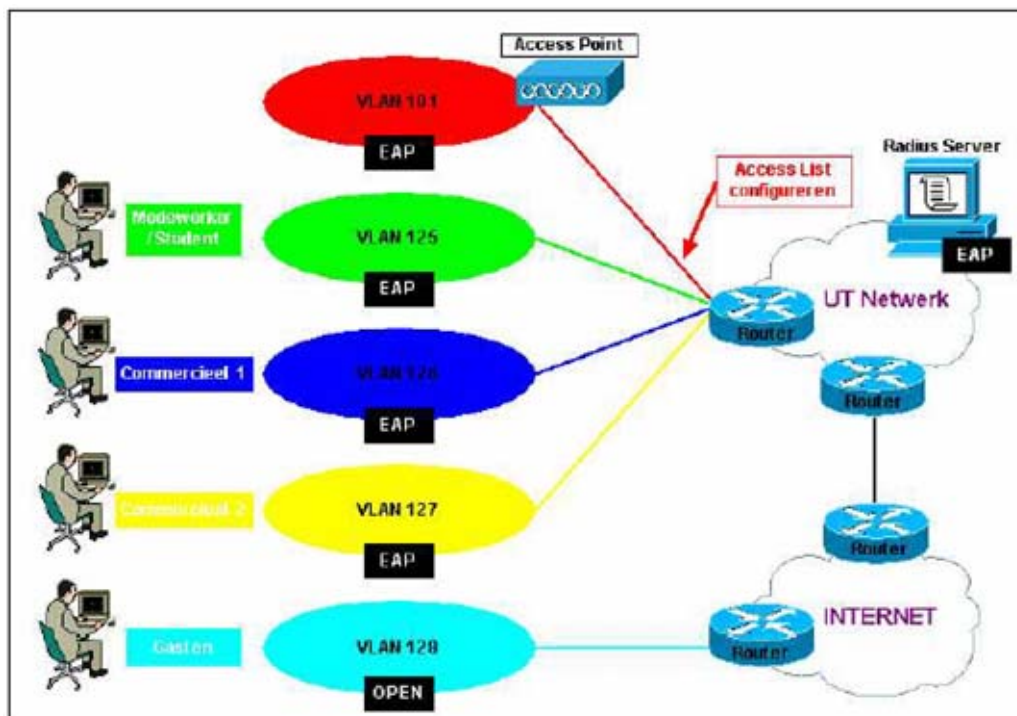


Figure 20: Network structure

2.5.1 Management measures

Usage agreements

All students have to sign a statement in which they certify *to use the computer and communication facilities available at the university for study purposes only in accordance with the guidelines set down by the university.*

There isn't such a statement for (all) staff members of the University.

2.5.2 Operational measures

The operational measures include but are not limited to the physical security of the access points. The access points are located in the faculties as well as on the campus. (There are also some access points in town and on the railway station for testing purposes but they fall outside the scope of this document). The access points in the faculties are, in most cases, attached on locations which are difficult to reach. The access points on the campus are 'hidden' in the ceilings.



Figure 21: Access point placement on the campus

2.5.3 Technical measures

In this paragraph I give a summarized version of the technical specification of the Utwente WLAN. The original document can be found on [COOK].

Appendix 1 consist the demands of the WLAN on which the implementation of the WLAN was based on.

WLAN@UT is protected using the IEEE 802.1x protocol in combination with TTLS (which is described in paragraph 2.3.3). For the time being a not secured (GUEST) network is also available. Registration of your MAC address is required for the use of the latter network.

The Authenticators (Access points)

The WLAN consists of 650 Cisco Aironet 1200 Series Access Points with 802.11b Mini-PCI radio modules. More documentation on this access point can be found on [CIS]. The access points are powered with power-injectors in the patch cases.



Figure 22: Cisco Aironet 1200 Series Access Points

The Cisco Aironet 1200 supports:

- 802.1x(§2.3.3)
- EAP(§2.3.3)
- EAP-Cisco (LEAP)(§2.3.3)
- EAP-TLS (§ 2.3.3)
- VPN (§ 2.3.1)
- Additional security functionalities based on draft standard 802.11i, like TKIP (MIC and Key Hashing) (§2.6.1)

The WLAN@UT cookbook [COOK] indicates the soft- and firmware versions below are installed on the access points. This means that the access points are at least updated to this version.

- Software version 12.01T
- Firmware version 5.02.12

The configuration of the Access Points is appended as *Appendix 2*.

The Supplicants

The Windows clients are using the Alfa & Ariss secure W2 client software. Open1x is available for Linux.

The authentication procedure using the secure w2 client is appended as *Appendix 5*.

The Cisco 6500 backbone switch

The Cisco 6500 is the default gateway for all the VLANs. This means that all the inter-VLAN traffic passes through this switch



Figure 23: The Cisco catalyst 6500 switch

The authentication-server

The University of Twente is using a RADIUS-server (Radiator) for Authentication, Authorization and Accounting (AAA).

A user database is necessary for the authentication of users, for instance a LDAP server or RADIUS-server with dial-up accounts. Middleware takes care of the association of various types of databases (SQL, LDAP, text file etc.).

Various radius-servers are connected using the “RADIUS proxy” technique. This technique makes the active RADIUS-server respond to the client while the actual check takes place on another server. This authentication goes through the Root RADIUS-server (See Image).

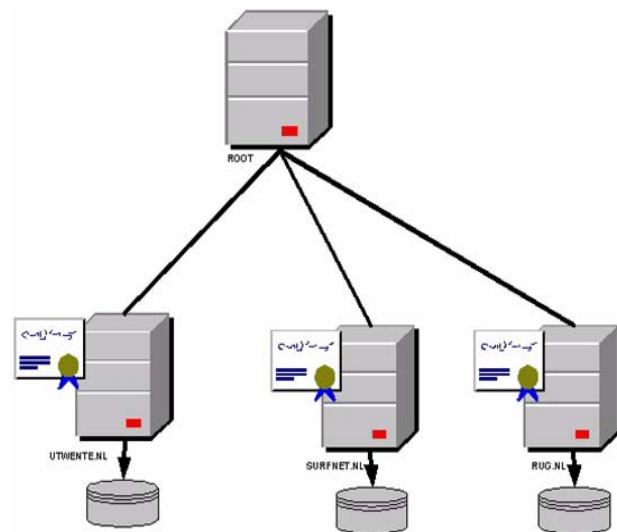


Figure 24: Radius proxy

A realm is used to discriminate between accounts in databases of the universities. The realm for the University of Twente is “utwente.nl” and for Surfnets is “surfnet.nl”.

According to the documentation the access point uses a 40 bits WEP key for the encryption of multicast and broadcast traffic. The client doesn’t have to store this key because it is sent to the client in the EAP authentication.

VLAN 1 (WLAN) is using a separate IP subnet in which only the access points and the RADIUS servers are included. The VLAN transport (tagging) is 802.1q based configured on the switches. The 802.1q standard defines the operation of VLAN Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure.

2.5.4 Knows security issues on this implementation

Certain releases of Cisco Aironet 1200 Series access points allow remote attackers to reboot devices by sending a specially crafted URL. Repeated exploitation of this HTTP GET command can lead to prolonged service interruption.

The vulnerability has been fixed in Cisco IOS software release 12.2(11)JA1 or later.

Other known vulnerabilities are:

- No authentication of management frames (assoc, disassociate etc)
- RADIUS-server failure causes the whole network to fail (single point off failure).

2.6 Under development (state-of-the-art solutions)

This paragraph describes the state-of-the-art solutions for WLAN security. The solutions described below can solve all known wireless attacks except the DoS attacks.

2.6.1 Temporal Key Integrity Protocol (TKIP)

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for WLANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 WLANs. TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism, thus fixing the flaws of WEP.

Before TKIP, it was possible to perform a known ciphertext attack on WEP after collecting a large number of packets. TKIP significantly mitigates the WEP key derivation vulnerability but does not provide complete resolution for the weaknesses.

Per-packet key mixing

TKIP generates a base key that is mixed into the per-packet key. Each time a wireless station associates to an access point, a new base key is created. This base key is built by hashing together a special session secret with some random numbers (called nonces) generated by the access point and the station as well as the MAC address of the access point and the station. With 802.1x authentication, the session secret is unique and transmitted securely to the station by the authentication server. TKIP uses the IV and the base key to generate a new key through a hash. This results in a new key for every packet.

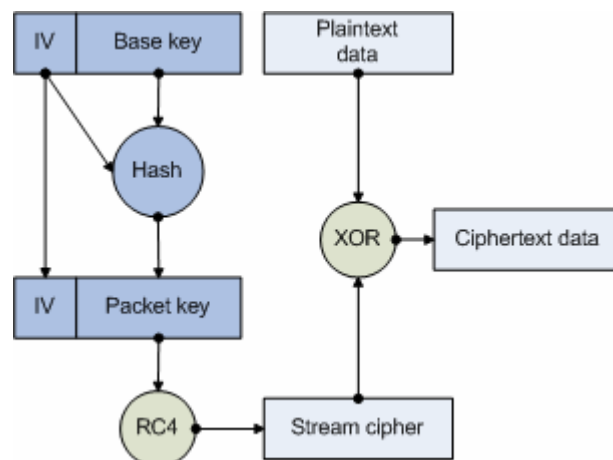


Figure 25: Key generation with TKIP

The message integrity check

The MIC (Message Integrity Check) is an additional 8 byte field which is placed between the data portion of an 802.11 (WiFi) frame and the 4 byte ICV (Integrity Check Value). WEP appends a 4-byte ICV to the 802.11 payload. The receiver will calculate the ICV upon reception of the frame to determine whether it matches the one in the frame. If they match, then there is some assurance that there was no tampering. Although WEP encrypts the ICV, a hacker can change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver. WPA solves this problem. Where the ICV protected only the packet payload, the MIC protects both the payload and the header.

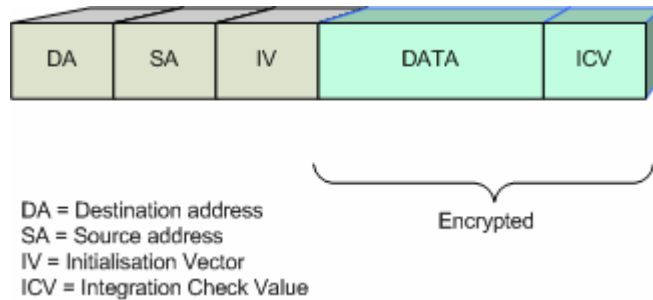


Figure 26: WEP encrypted packet

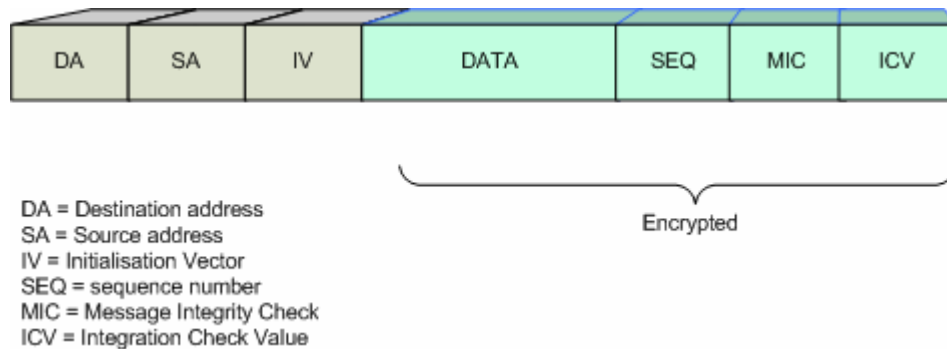


Figure 27: WEP encrypted packet with TKIP

The MIC is based on Seed value, Destination MAC, Source MAC, and payload, any change to these will change MIC value. More information about MIC can be found on [MIC].

IV sequencing

Each packet transmitted using TKIP has a unique 48-bit serial number that is incremented every time a new packet is transmitted and used both as the Initialization Vector and part of the key. Putting a sequence number into the key ensures that the key is different for every packet. This solves another problem of WEP, called "collision attacks", which can occur when the same key is used for two different packets. With different keys, there are no collisions.

Initially, 802.11i will provide Temporal Key Integrity Protocol (TKIP) security that you can add to existing hardware with a firmware upgrade. Upgraded units should be backward-compatible with hardware that still uses WEP. Sometime later, new chip-based security that uses the stronger Advanced Encryption Standard (AES) protocol will replace TKIP, and the new chips will probably be backward-compatible with TKIP.

2.6.2 Wifi Protected Access (WPA)

WPA was created by the WiFi alliance in 2002 – in part out of impatience with the slow-moving 802.11i standard. WPA includes Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms. The combination of these two mechanisms provides dynamic key encryption and mutual authentication.

Unfortunately, the easiest way to use WPA actually makes it easier to crack than WEP. When 802.1X authentication is not used in WPA, a simpler system called Pre-Shared Key (PSK) is. PSK offers a long-lived password that everyone who wants to connect to the WLAN has to know.

With WPA-PSK, if you don't make your password long, you're susceptible to an offline dictionary attack where an attacker grabs a few packets at the time a legitimate station joins the wireless network and then can take those packets and recover the PSK used. Of course, this type of attack depends on people choosing poor passwords.

In a home or Small Office/ Home Office (SOHO) environment, where there are no central authentication servers or EAP framework, WiFi Protected Access runs in a special home mode. This mode, also called Pre-Shared Key (WPA-PSK), only requires a **single password** entered into each WLAN node (Access Points, Wireless Routers, client adapters, bridges). As long as the passwords match, a client will be granted access to a WLAN.

As with WEP, wireless cracking tools exist that are specifically designed to recover the PSK from a WPA-protected network.

WPA with 802.1x authentication - sometimes called WPA-Enterprise - yields a very tight network.

The intrinsic encryption and authentication schemes defined in WiFi Protected Access may also prove useful for Wireless Internet Service Providers (WISPs) offering WiFi public access in “hot spots” where secure transmission and authentication is particularly important to users unknown to each other. The authentication capability defined in the specification enables a secure access control mechanism for the service providers and for mobile users not utilizing VPN connections.

An issue that WPA does not fix yet is potential Denial of Service (DoS) attacks.

2.6.3 802.11i (WPA2)

The long-anticipated 802.11i specification was finally ratified by the IEEE in June 2004. The new specification offers significant improvements over the old standard (WEP). It describes the encrypted transmission of data between systems of 802.11a and 802.11b WLANs. It defines new encryption key protocols including the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES). further improvements are:

- Authentication of management frames. This prevents simple session hijacking.
- Authentication of EAP-success messages prevents simple MitM attacks

WPA2 is backwards compatible with WPA.

2.7 Summary

The new 802.11i standard described in the paragraphs above does solve almost all known weaknesses in wireless implementations used today. The hardware used today doesn't support this new standard and should be updated or replaced to make use of it. Since WPA was designed to be compatible with 802.11i later on, it has been a good choice of a lot of companies to upgrade their systems to WPA.

3 Weaknesses of the wireless network

This chapter starts with the results of a brief wardrive session in Enschede which shows that a lot of the WLANs in the area are not or barely protected. Next I focus on the implementation of the Utwente wireless network and perform a number of tests on this network. The chapter concludes with a conclusion based on the found results.

3.1 Attacks on a wireless network

Most attacks follow a five phased approach which are described in this paragraph. The first three phases are more-or-less followed in the next paragraphs.

Phase 1: Reconnaissance

In this phase information is collected, like IP addresses, available servers and their functions and so on. A variety of techniques can be used here including social engineering, dumpster diving, searching an organization's own web site, mapping access points with undetectable tools as kismet or even physical break-in.

Phase 2: Scanning

After the first phase, an attacker wants to make an inventory of the systems on the network. If he has internal access to the network already (as all students do) he can scan the network using ICMP pings and TCP/UDP packets (many networks block ICMP messages). Further scanning includes the use of traceroute, Nmap and vulnerability scanners like Nessus.

Phase 3: Gaining Access Using Application and Operating System Attacks

At this time the attacker wants to get access to the target systems. Using exploits, password guessing techniques, sniffers (like Snort, Tcpdump or Ethereal) or session hijacking.

Phase 4: Maintaining Access

After gaining access, the attacker will try to maintain that access. To achieve this, techniques based on Trojans, backdoors, and rootkits are used.

Phase 5: Covering Tracks and Hiding.

This final phase includes altering event logs and hiding files (e.g. attack tools)

3.2 Pentests vol. 1: A quick wardrive session

Wardriving is an activity consisting of driving around with a laptop, detecting wireless networks. Whole communities work together to map all the access points in a certain area. I took screenshots below on this page from a website that is designed to map all the wireless access points in the Netherlands.



Figure 28: Access points in Enschede

In this test I will drive around in Enschede and on the University campus to detect wireless networks in the area and perform controlled penetration tests on these networks. The results of these tests will give us an indication of most occurring security shortcomings. This chapter will discuss these shortcomings and illustrate how to prevent them.

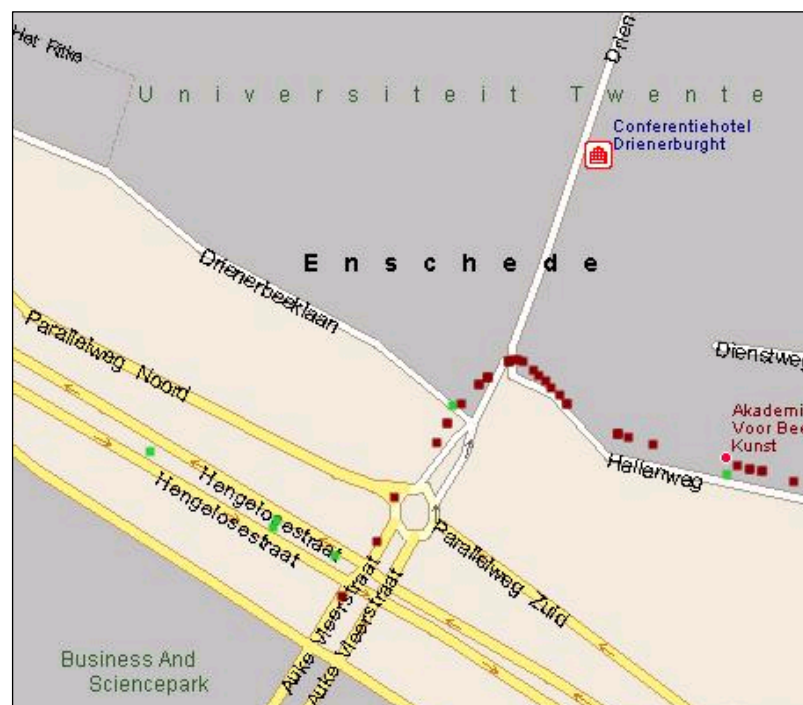


Figure 29: Access point in Enschede in detail

3.2.1 Preparing for the pentests

The hard- and software below was used for the pentests. See chapter 2.2.2 for a description of the used tools.

Hardware used for the pentests:

- Laptop with both Linux and Win2k installed
- Wireless NIC which supports monitor mode

Software used:

- Netstumbler 0.4
- KMAC
- Ethereal
- Look@LAN
- (Lopthcrack)
- LANguard
- NMAP
- Air_jack

3.2.2 Phase 1: Reconnaissance

A wise thing to do before any wardriving or similar activity is to spoof your MAC-address so the fake MAC-address will be stored in the logfiles on the access points and other systems you connect to instead of your own unique MAC -address.

In Linux, this can be performed with a simple *iwconfig* command. In Windows I have a few tools at my disposal such as *Kmac* or *Smac*. At this time I used *Kmac*. The tool works very straightforward as can be seen in Figure 30.

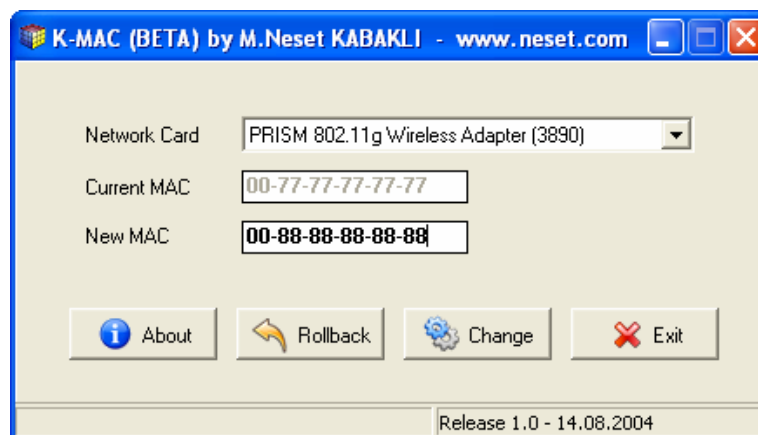


Figure 30: Kmac spoofs our MAC-address

In order to penetrate a WLAN, an access point must be located. Some access points broadcast frames that contain information about the WLAN which can be exploited by Netstumbler. Note that Kismet can also detect access points which don't send these broadcast frames. For this demonstration Netstumbler was used for the detection of the access points because Netstumbler has a nice feature to determine the exact location of the access points. Once Netstumbler is executed, it starts sending out broadcast probes at a rate of once per second. When an access point responds to the probe, Netstumbler alarms and reports information extracted out of the 802.11b frames such as SSID, MAC address, channel, signal strength and whether WEP is on. A Screenshot of the Netstumbler results is shown below. The detailed results of the scans can be found in *appendix 3*.

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
00028AA99454	tsunami		2	11 Mbps	Ambit	AP	WEP		-87
0060B301ADF2	Sitecom		6	54 Mbps	Z-Com	AP			-90
000DED2ECE2B	ProRail		11	11 Mbps	Cisco	AP			-82
000F662508FB	linksys		11	54 Mbps	Linksys	AP			-81
0010E7F5D1E1	Enschede_Oost.##		1	11 Mbps	Breeze...	AP			-89
000DBC25EFF5	ProRail		6	11 Mbps	Cisco	AP			-86
000D659BAD07	ProRail		1	11 Mbps	Cisco	AP			-76

Figure 31: Detected access points with Netstumbler

The first column in the Netstumbler table shows us the MAC-address of the detected access point. The SSID is shown in the second column. Further useful information is the Vendor (remember the usage of default passwords) and encryption settings. A blank field in the encryption column means that encryption is disabled. This can also be concluded from the absence of the small lock in the dot before the MAC-address.

As indicated before I could also have used *Kismet* to detect the SSID of wireless networks which would show me the SSID of networks that 'hide' their SSID as well. Another useful tool to detect the SSID of a network is the *Airjack suite* [AIRJ]. The SSID is not removed from all management frames. Reauthenticate and reassociate frames will contain the SSID value. Thus, a network with roaming hosts will not benefit from the closed SSIDs at all. Airjack sends a deauthenticate frame to one or more hosts on the closed WLAN and captures the SSID from the management frames.

```
kaa:~# essid_jack -b 00:07:85:b3:72:f1 -c 11
Got it, the essid is (escape characters are c style):
"Invisible_SSID"
```

To detect the SSID of a 'closed' network one could also use the OUI, which is the first three bytes of the MAC-address (of the access point), to find out the access point manufacturer and check the default ESSID values for the access points produced by this particular vendor and supporting closed SSIDs.

Most access points on the Utwente campus are Cisco access points with WEP encryption enabled using channel 1, 6 or 11 and SSID 'WLAN'. Other access points which were detected on the campus are:

SSID	Channel	encryption	Manufacturer
WLAN-TI	3, 4, 8, 10 or 13	WEP	
quadapt and TI4GB	5, 6 and 10		Proxim
sjeeskonijn	7		BenQ
unknown	1, 3 and 7		Cisco

Table 3: Detected SSIDs on the campus

Outside the campus a lot of access points without encryption enabled were detected.

I decided to select one of the detected access points outside the campus for some further testing. For the next step I used Netstumbler to determine the exact location of the access point as indicated earlier. Netstumbler can produce a visual representation of the signal strength which I can use (in combination with a directional antenna) to come as close to the access point as possible. Note that the exact location of the access point also can be recorded using a GPS system. A screenshot of such a representation is shown below.

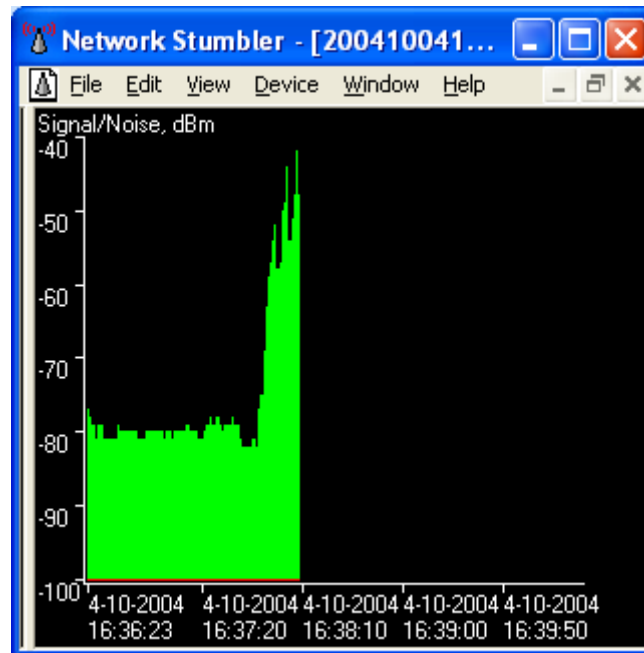


Figure 32: Signal strength measurement in Netstumbler

3.2.3 Phase 2: Scanning

With the access point located, it was time to gather information to see if the network was vulnerable. Some WLAN administrators set up a DHCP server for the WLAN segment that will assign a wireless NIC an IP address and default gateway. Since the selected network didn't have MAC filtering, or encryption enabled, I could almost enter this network immediately. Furthermore I could already view all network traffic without even joining the network using *Kismet*. (Due to the passive nature of this attack it cannot be detected and therefore capturing traffic with *Kismet* actually belongs in the first phase.

If the wireless NIC is *associated* to the access point (layer 2) but do not have an assigned IP address (layer 3) for the local WLAN segment, they cannot participate on the TCP-IP WLAN. In order to have routing privileges or Internet connectivity, the wireless NIC needs a layer 3 IP address and default gateway. Gaining an IP address can be accomplished with Ethereal/TCPdump by sniffing the air medium for packets containing the vital IP information.

In this situation the DHCP-server nicely provided us with an IP-address. However I will discuss a possible approach for the case you don't get an IP address assigned.

In that case a logical step would be the sniffing of the network traffic using *Kismet*. This tool stores all intercepted traffic for later analysis and shows us vital IP information immediately. A Kismet scan of our small wardrive session is shown below.

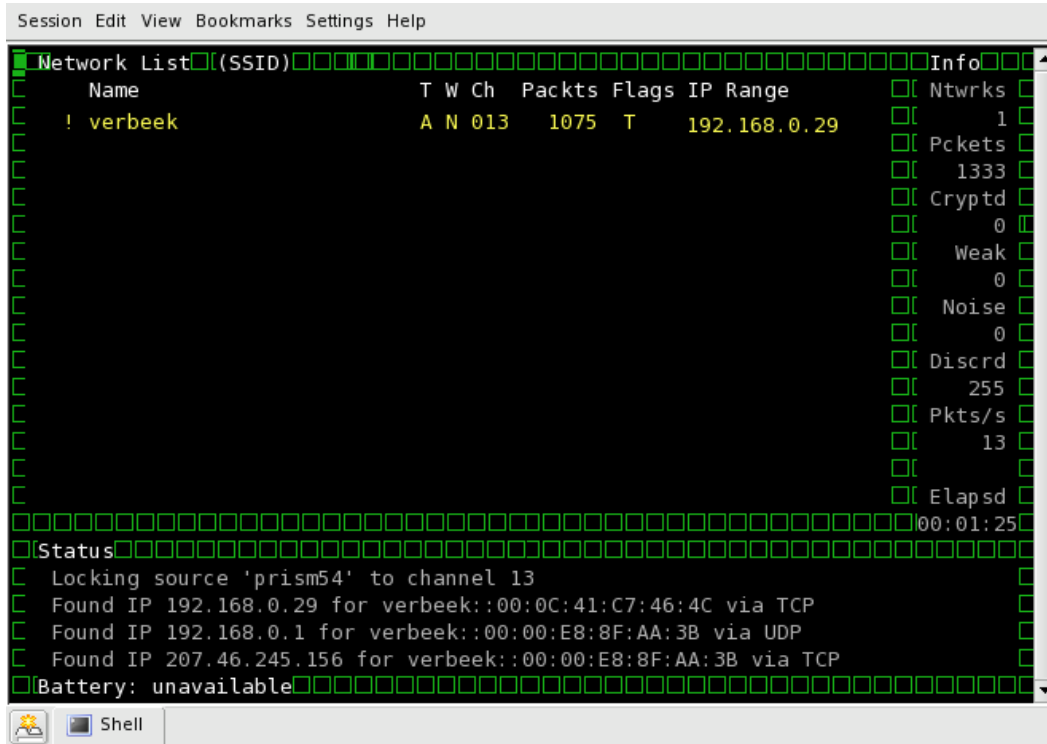


Figure 33: Sniffing packets with Kismet

More information about the network can be viewed in Kismet as can be seen here:

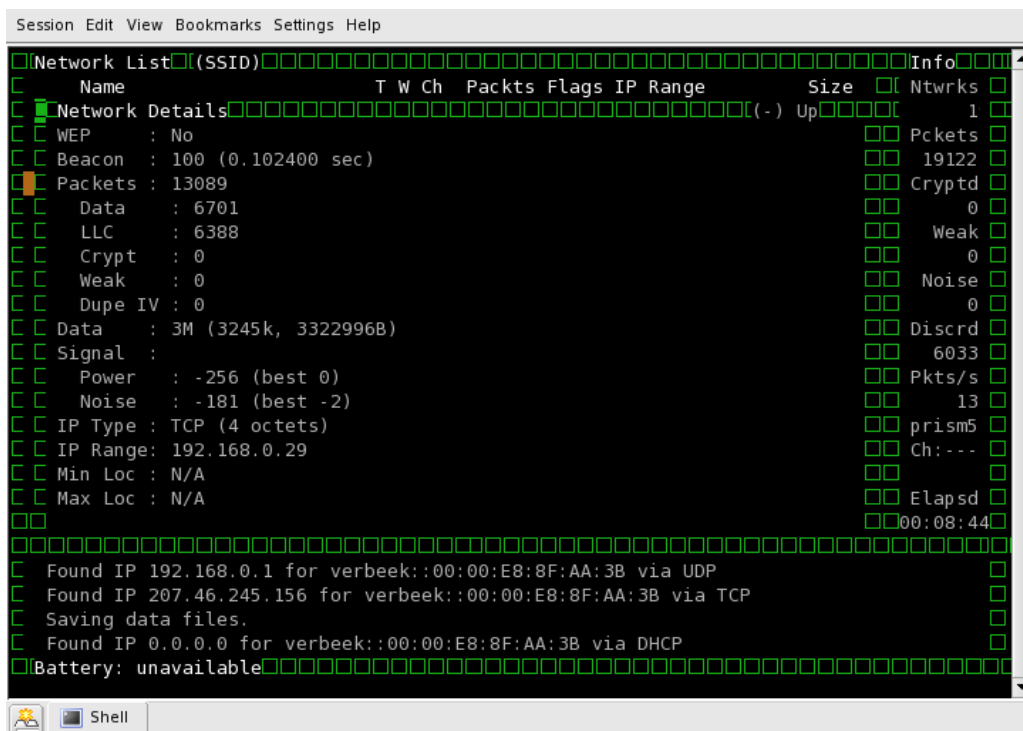


Figure 34: Network details from Kismet

The recorded packets from *Kismet* can be viewed with *Ethereal*. At the moment I performed my Kismet scan, our victim was using MSN messenger. Note that the stream below has been filtered from beacon and other not interesting packets.

Source	Destination	Protocol	Info
207.46.108.31	192.168.0.29	HSNNS	[TCP Previous segment lost] ACK 21
207.46.108.31	192.168.0.29	HSNNS	HSG [redacted]@hotmail.com [redacted]
207.46.108.31	192.168.0.29	HSNNS	[TCP Retransmission] MSG [redacted]@hotmail.com [redacted]
207.46.108.31	192.168.0.29	HSNNS	[TCP Retransmission] MSG [redacted]@hotmail.com [redacted]
207.46.108.31	192.168.0.29	HSNNS	HSG [redacted]@hotmail.com [redacted]
192.168.0.29	207.46.108.31	TCP	[TCP Previous segment lost] 3319 > 1863 [ACK] Seq=1926 Ack=1956 Win=16108 Len=0
207.46.108.31	192.168.0.29	HSNNS	HSG [redacted]@hotmail.com [redacted]
192.168.0.29	207.46.108.31	TCP	3319 > 1863 [ACK] Seq=1926 Ack=2662 Win=17520 Len=0
207.46.108.31	192.168.0.29	HSNNS	HSG [redacted]@hotmail.com [redacted]
192.168.0.29	207.46.108.31	TCP	3319 > 1863 [ACK] Seq=1926 Ack=3385 Win=16797 Len=0
207.46.108.31	192.168.0.29	HSNNS	C&IY\231\214[6]bs(\213\2359>i\036n\B'M\213fi0F~L9súq\216\034± \026Qx\$\'200'\02
207.46.108.31	192.168.0.29	HSNNS	'P\204x\231IK\z\223\234\003bîsûët*02ñ;X\004Ci5Wúáñp\$\'016APi"i\210\220\004c\035
207.46.108.31	192.168.0.29	HSNNS	[TCP Retransmission] 'P\204x\231IK\z\223\234\003bîsûët*02ñ;X\004Ci5Wúáñp\$\'016A
207.46.108.31	192.168.0.29	HSNNS	HSG [redacted]@hotmail.com [redacted]
207.46.108.31	192.168.0.29	HSNNS	\023pã0úî0Çîñ\205K\227>ÄQRO\006rRD\2105Êtuêls\217Ê'ã\220cFsc0dI\0301\2071ià\003
207.46.108.31	192.168.0.29	HSNNS	[TCP Retransmission] \023pã0úî0Çîñ\205K\227>ÄQRO\006rRD\2105Êtuêls\217Ê'ã\220cF
207.46.108.31	192.168.0.29	HSNNS	[TCP Retransmission] \023pã0úî0Çîñ\205K\227>ÄQRO\006rRD\2105Êtuêls\217Ê'ã\220cF

Figure 35: Examining the captured packets with Ethereal

From the *Kismet* and *Ethereal* results I concluded that IP addresses used where in the 192.168.0.xxx range. I discovered the IP addresses **192.168.0.29** and **192.168.0.1**.

I assume that the 192.168.0.1 address is the address of the router and/or access point

After the IP-range has been determined, an IP-address can be assigned manually, and the network can be entered. (In this situation I already received an IP-address from the DHCP server)

Protocol filtering is harder to bypass. Unfortunately for system administrators and fortunately for attackers, very few access points on the market implement proper protocol filtering and they tend to be high-end, expensive devices. The main attacks against networks protected by protocol filtering are attacks against the allowed secure protocol. A good example of such insecurity is the well-known attack against SSHv1 implemented in *Dsniff*.

Wondering whether **192.168.0.29** was the only online system I used *Look@LAN* to get an overview of the systems online. *Look@LAN* uses a simple ping-scan to detect online systems. Results of such a scan are shown below.

IP Address >	Status	Distance	O.S.	HostName	NetBIOS Name	NetBIOS User	SNMP	Trap
192.168.0.1	ONLINE	Same LAN	NOT WIN	my.router	-	-	-	-
192.168.0.80	ONLINE	Same LAN	WINDOWS	RUBEN	RUBEN	ADMINISTRATOR	-	-
192.168.0.29	ONLINE	Same LAN	WINDOWS	RubenLaptop	RUBENLAPTOP	RUBENLAPTOP	-	-
192.168.0.213	ONLINE	Same LAN	WINDOWS	LAPTOP-MARIJN	LAPTOP-MARIJN	(n/a)	-	-

Figure 36: Subnet scanning with Look@LAN

Another online system was found with IP address 192.168.0.80. For now I will continue focusing on the system found earlier.

The final step in this phase is scanning for vulnerabilities and open ports. Below results from an Nmap scan are shown in Figure 37. The results from *Languard network security scanner* are shown in Figure 38. This reveals already a vulnerability that possibly can be exploited to compromise the system.

```
[root@localhost kaa]# nmap -O 192.168.0.29

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-10-07 01:03 EDT
Interesting ports on 192.168.0.29:
(The 1655 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Professional
or Advanced Server, or Windows XP
Nmap run completed -- 1 IP address (1 host up) scanned in 15.228 seconds
[root@localhost kaa]#
```

Figure 37: Portscanning with Nmap

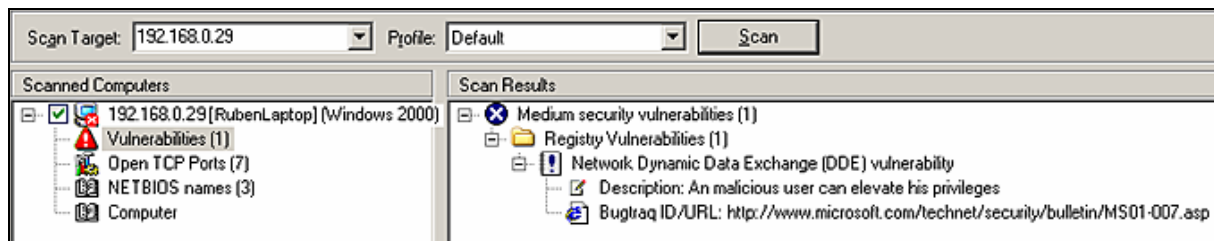


Figure 38: Searching for vulnerabilities with LANguard

In contrast to our sniffing before, port scanning and vulnerability scanning will alert a cautious user. If the user targeted is using a firewall or other detection system, he will undoubtedly be notified of out scan. In this situation I didn't suspect any of these systems; however one should be aware of the possible detection at this point.

3.2.4 Phase 3, 4 and 5: Access to the WLAN

The third phase concerns gaining access to the target systems, using techniques as password guessing, the use of exploits, and other techniques. The first thing I tried was the use of default passwords for the access point. Unfortunately for me, the user did change the address. That this 'technique' is worth trying proves the results of the attempts a few houses further where I actually gained access to the access point trying the default passwords. *Appendix 4* contains screenshots of these attacks.

In this case the network is not protected using WEP. In the section dealing with WEP cracking tools, four major ways of attacking WEP are described:

- Brute-forcing
- FMS attack
- IV/WEP key replay
- Bit flipping

From the Languard results I knew the target was using a windows 2k system. One of the well-known overlooked 'features' of a windows 2k system is the presence of the so called admin-shares. These shares are hidden, but freely available when the user has *file and printer sharing* enabled. This allows us to completely search the system. One of the interesting files may be the *sam file* which contains the user account information and passwords. This file is stored in the `%systemroot/system32/config` directory, but can't be copied because it's locked by the operating system. Windows keeps a copy of this file in the `%systemroot/repair` dir which I could copy for further examination.

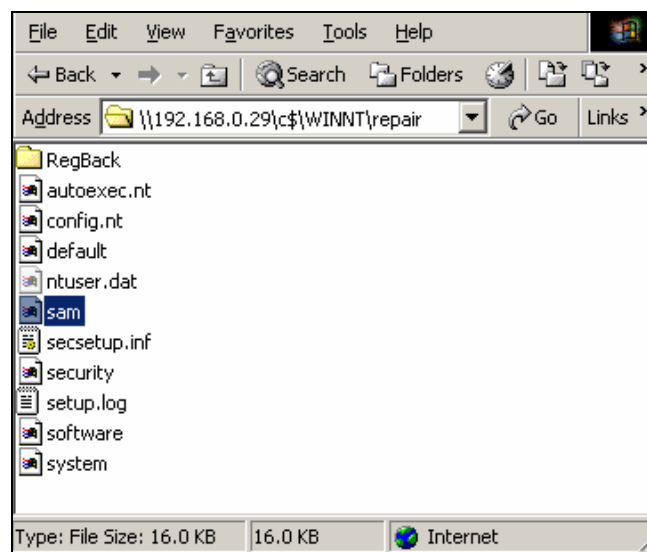


Figure 39: Admin shares victims system

All steps before were legal actions by the Dutch law. I captured an unencrypted data stream, performed some scans on the network and viewed shared folders on the open network. Next logical step for a hacker would be copying the sam-file and crack it with Lophtcrack or similar tool as indicated before. However, copying files, or opening private documents or emails is illegal and violates the victim's privacy and therefore this step concludes the attack.

3.3 Pentests vol. 2: Attacks on the Utwente WLAN

I distinguish between two types of attackers.

1. outsiders
2. students/employers with valid account

3.3.1 Preparing for the pentests

Hardware used for the tests:

- Laptop with two wireless NICs (at least one allowing access point mode) and both Linux and win2k installed (the attackers system)
- DB-9 to RJ45 serial cable
- Cisco 1200 Access point connected to RADIUS server and user database
- Wireless client system with valid account (the victims system)

Software used during the tests:

- Server certificate
- Secure W2 client software
- Ethereal
- Kismet
- Cain version 2.5b56

3.3.2 Phase 1: Reconnaissance

This part of the research focuses on the available wireless systems on the campus and describes the differences between these systems as well as all the detail that can be found about these systems. This information is collected by visiting websites, scanning the area with *Kismet*, social engineering and not unimportant visiting the Utwente website and other public available documents.

Much of the collected information about the wireless network of the University is summarized in paragraph 1.1. Only the additional information is described here.

The networks below are detected on the campus using *Kismet*:

- **WLAN** - This is the main WLAN and is protected using the 802.1x standard as stated before.
- **INF-WLAN** - This LAN covers the computer science building and is mainly used for testing purposes. This LAN is not protected. I used *Ethereal* to examine the data captured with *Kismet* but found no sensitive data. There was very little data traffic by a small amount of users during the captures. It looks like this network is indeed used for testing purposes only. MAC-filtering is disabled in this network. The used IP-range for this WLAN is 130.89.15.xxx and DHCP is disabled
- **RES-WLAN**- An access point with this SSID was detected in the computer science building. Viewing the data stream it looks like this is also a test network just as the last one. Also in this network MAC-filtering is disabled. The used IP's are in the range 130.89.144.xxx and DHCP is disabled

- **GUEST** - This network is for guests or other user who cannot use the 802.1x authentication. The use of encryption is disabled on this network and therefore it shouldn't be used to send confidential data. Usage of the network requires a permanent or temporary registered MAC-address. However as stated before a registered address is easily discovered by capturing the (not encrypted) traffic of a legitimate user. This address can subsequently be used to access the network. SSID broadcasting is disabled for this network.

The risks involved in using this network are well known and also indicated in the user manual [UTG] available.

- **TI4GA, TI4GB and quadapt** - These networks have encryption enabled and don't have an open authentication allowing us to join them. There is an acceptable change they were installed by students or employees and therefore don't use dynamic key rotation. Assuming that this is the case, this could result in a successful key-break by the use of Aircrort, WEPcrack, WEPlap or a similar tool. Investing this possibility might take several days depending on the amount of traffic, and even if the keys can be broken, and the assumption is proven to be true, this won't give me much more information as I already have now. What is important here is the fact that there are possibly so called 'rogue access points' plugged into the network which can be a welcome less secure entrance for an outsider to enter the network behind it.

3.3.3 Phase 2: Scanning

An outsider doesn't have many options here. All the traffic is encrypted and the 802.1x technology takes care of the authentication. The only thing an outsider can conclude here is that there are a lot of access points and a lot of users. More information cannot be collected without an active attack on the network. Of course I could check the whole area for misconfigured access points and/or rogue access points, but this would be a very time-consuming job with little contribution to the project.

On the other hand, the attacker that possesses a valid account can find some more detailed information here. A ping scan in the subnet leads to a huge amount of clients, in the 130.89.13x.xxx range.

Further information can be derived from the operating system as shown here from the windows XP.

Vulnerability scans of the wireless clients belong in this part of the test as well. These are discussed in the next paragraph in combination with one of the actual attacks to improve the readability of the document.

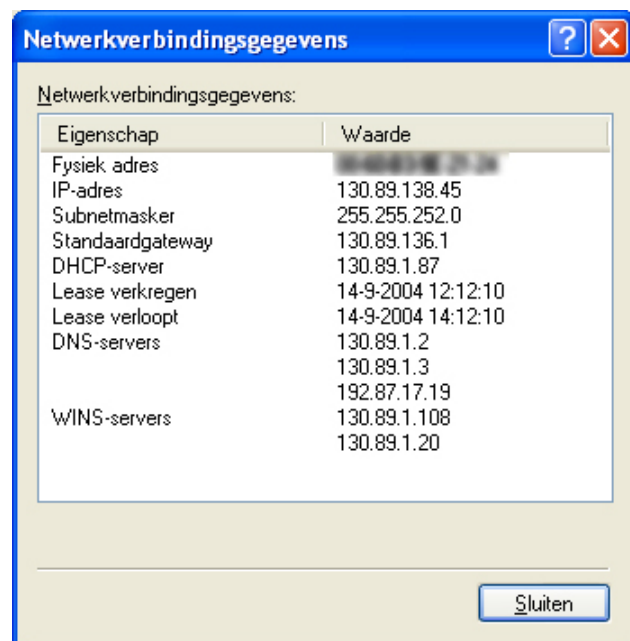


Figure 40: Network details from winXP

3.3.4 Phase 3, 4 and 5: Access to the WLAN

In this part of the test I distinguish six types of attacks. The first three are based on techniques that could be performed by outsiders. The other three techniques require additional possibilities such as access to a valid network account.

Accessing the wireless network as an outsider

An outsider is limited to attacks on the data stream between client and authenticator, or attacks on the accessible hardware (the access points). The next three attacks are geared to these possibilities.

1. MitM attacks

I investigated the possibility to place my own access point between the legitimate access point and the victims system and lure a wireless client to connect to my system. Because an outsider wouldn't have a valid account at his disposal, I examined the possibility to replay the authentication messages of the victim to gain access to the access point and possibly decrypt the message stream as well. The results of this attack are described in paragraph 3.3.4.1.

2. Session hijacking

I investigated the possibility to disassociate an authenticated client and takeover the open connection to the Internet. The results of this attack are described in paragraph 3.3.4.2

3. Attacks on the hardware

The goal of this attack was to gain access to the access points themselves and change the configuration in order to gain access to the network and/or clients connecting to this network using this or other access points. Some social engineering was used to determine whether attackers would experience any difficulties to access the hardware on the campus. The results of this attack are described in paragraph 3.3.4.3

Accessing the network as a student or employee

Attacks 4, 5 and 6 are based on the use of information and possibilities a student or employee has.

4. Rogue access points

Students or employees can install an access point on the wireless or wired network using their own user credentials. Protection of the network traffic between this access points and wireless clients would depend on the access point configuration and be independent of the chosen authentication method to the University network. This test aims on the possibility that normal users accidentally connect to such an access point and subsequently are exposed to risks without their knowledge. The results of this attack are described in paragraph 0

5. Social engineering

According to information on the ITBE website the student ID-card is required to prove your identity while changing your password at the ITBE helpdesk. I visited the helpdesk and tried to talk them into changing or resetting the password for 'my' account without such a card. The results of this attack are described in paragraph 3.3.4.5

6. Wireless and wired clients

People are almost always the weakest link when it comes to security. People write down their passwords on sticky notes and tape them on their monitor or on top of their agenda. They use their passwords in insecure places or store them on unprotected systems. In this part of the project I looked at the vulnerabilities caused by users because of unwise behavior or lack of knowledge and awareness. The results of this attack are described in paragraph 3.3.4.6

3.3.4.1 A MitM attack

Test goal

To decrypt intercepted data and gain access to the access point.

Test procedure

Place an unauthorized access point (with a stronger signal, and same SSID) between the legitimate access point and the victims system, and fool the victim to connect to my system. Next replay the authentication messages of the victim to gain access to the access point.

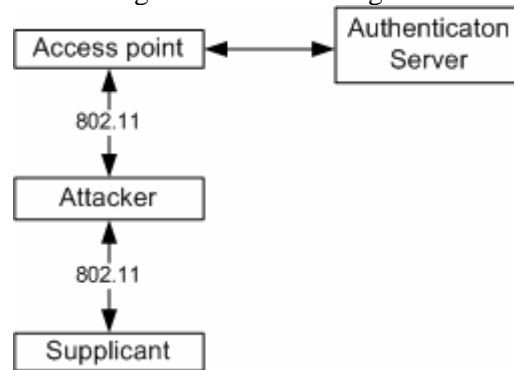


Figure 41: MitM attack

Used hard- and software

For the victims machine I used a windows 2k machine with secure W2 version 2.0.0 and a Linksys WPC54G wireless NIC. The attacker's system was a Mandrake 10 Linux pc with an Intersil internal wireless NIC to communicate with the access point and a Senao NL-2511 CD PLUS-EXT2 NIC with external antenna to act as access point. Ethereal was used to view the network traffic.

Results

According to various papers and articles such as *An Initial Security Analysis of the IEEE 802.1X Standard* [ARBA] this attack should be possible in the current implementation. Concerning to this and other documents 802.1x was conceived as an asymmetric protocol, allowing the network to authenticate the user, but not allowing the user to authenticate the network. Therefore according to the documents, an attacker could fool the victim into connecting with it rather than with a legitimate access point. The attacker could then play "Man-in-the-Middle", passing data between the mobile station and the legitimate access point, and eavesdropping all the while.

During the test I could fool the victim's system into connecting with the unauthorized access point instead of the legitimate access point but it was impossible to forward and authenticate to the access point.

Conclusion

The vulnerability described doesn't apply to the EAP-TTLS protocol. The use of this protocol result in master keys on both station and access point for encrypting data between the two. The master keys are intimately bound to the authentication that preceded them. This eliminates the man-in-the-middle threat. Because the attacker was not authenticated to either party, he has no master key and can't get one. Therefore, even if it were able to pass data between mobile station and access point, it would not be able to decipher that data.

3.3.4.2 Session Hijacking

Test goal

To disassociate an authenticated client and takeover the open connection to the Internet.

Test procedure

Pose as the access point to the victim, and pose as the victim to the access point. First, fake a packet to the victim as if it came from the access point, telling the victim to “disassociate”, or drop its connection. Then, “hijack” that connection, using the victim’s MAC-address to fool the access point into exchanging data. In the first run I used a wireless network card to act as access point; in the second run I used a Cisco access point.

Used hard- and software

For the victims machine I used a windows 2k machine with secure W2 version 2.0.0 and a Linksys WPC54G wireless NIC. The attacker’s system was a Mandrake 10 Linux pc with an Intersil internal wireless NIC to communicate with the access point and a Senao NL-2511 CD PLUS-EXT2 NIC with external antenna to act as access point in the first run and a Cisco Aironet 1200 access point in the second. The Software used is Ethereal and WEPWedgie

Results

I could successful spoof the MAC-address of the access point and disassociate the connected client. Next I spoofed the MAC-address of the client and tried to communicate to the access point. In this stage I experienced the same problems as with the MitM attack.

Conclusion

An attacker could forge a “disassociate” packet to disconnect the victim, but he could not hijack its connection. To hijack the connection he would need the correct master keys. To get those he would need to have been authenticated.

3.3.4.3 Attacks on the hardware

Test goal

To gain access to the WLAN hardware and change the configuration.

The results of this test should provide an answer to the questions below:

- Is it possible for an attacker to reset the access point to the default settings and/or change the access point's configuration?
- Does this type of attack provide the attacker with illegitimate possibilities such as sniffing traffic from clients?
- Can the attack be detected?

Test procedure

Try available methods to change or reset the configuration. Methods to change the access point's configuration in general are telnet, the web interface, SNTP or a serial connection. Furthermore I considered: the possibilities below:

- According to the user manual, it is possible to reset the AP using the mode button
- If the firmware isn't updated to the latest version, known security bugs can possibly be exploited.
- Using default passwords can lead to illicit access.

Used hard- and software

For the victims machine I used a windows 2k machine with secure W2 version 2.0.0 and a Linksys WPC54G wireless NIC. The attacker's system was a Mandrake 10 Linux pc with an Intersil internal wireless NIC. The Software used is Ethereal, SecureCRT and Netstumbler 0.4.

Furthermore I used an access point of the same type and with the same configuration as used on the WLAN.

At the moment two different version of the Aironet 1200 access points are in use. Most of the access points are installed with the Vxworks firmware. Only a few access points in the WB building are using the (newer) IOS version of the firmware. In the future the firmware of all access points will be upgraded to the IOS version. Therefore I didn't waste time examining the Vxworks variant of the access point and focused on the IOS version immediately. Precise information on the access point is summarized in the table below.

Product/Model Number:	AIR-AP1220-IOS-UPGRD
System Software Filename	c1200-k9w7-tar.122-13.JA2
System Software Version:	12.2(13)JA2
Bootloader Version:	12.2(8)JA

Table 4: Access point configuration

Results

The easiest way to alter the configuration is to reset it as described below and then change it using the web-interface. I performed the actions from the Cisco manual below to reset the AP:

- Step 1** *Disconnect power (the Ethernet cable for in-line power) from the AP.*
Step 2 *Press and hold the MODE button while you reconnect power to the AP.*
Step 3 *Hold the MODE button until the Status LED turns amber (approximately 1 to 2 seconds), and release the button. All AP settings return to factory defaults.*

This indeed resets the access point to default settings, including the password and security settings. I don't expect this part to be a problem to cause any problems in the live network as well. The ITBE staff confirms in an interview that the access points can be reset using this

‘technique’. According to the ITBE staff a reset access point still gets an IP-address from the DHCP-server and allows clients to access the Internet. However these access points can be detected (with Cisco WLSE) which would possibly ends in the ITBE staff disconnecting the access point from the network. The ITBE staff could not indicate in what period of time they will react to such detection nor could they hand over documents which described the response for this incident.

With the access point reset to default settings, I had several options to change the configuration. The easiest way is to use a web-browser and navigate to the IP address of the access point. The default username and password “Cisco” can now be used to enter the administration menu.

Now I could enable WEP encryption, set the authentication method to “open”, switch the channel to 1, 6 of 11 and change the SSID to “WLAN”. This is described in the next section called “Installing rogue access points”.

Since the access point can easily be reset using the reset button it wouldn’t be of much use to investigate other ways to change the access point’s configuration (except for deriving the RADIUS key from the device).

As indicated before, other ways to connect to the access point are by means of a serial cable, using the Simple Network Management Protocol (SNMP) or a telnet session. A password is required for all these. Connecting using the command-line interface (CLI) such as SecureCRT through a serial cable (DB-9 to RJ-45) requires the settings shown in Figure 42.

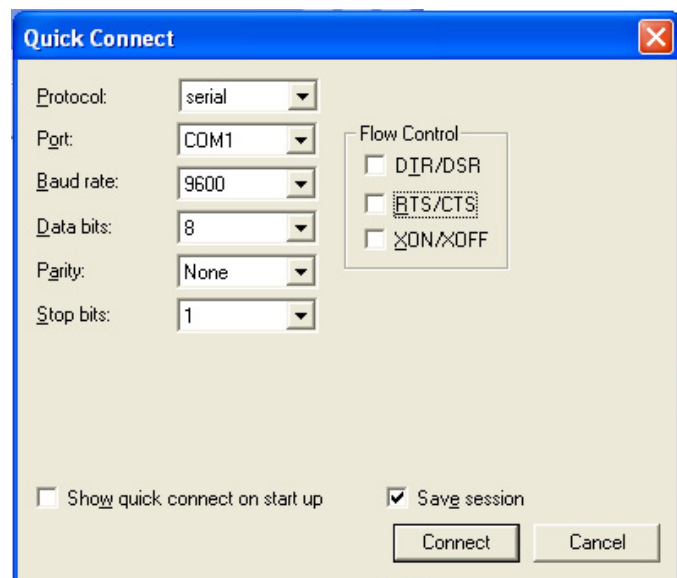


Figure 42: CLI settings

To demonstrate this attack is also applicable for an outsider, provided with a convincing ITBE ID-card, I visited three groups of (unknown) students on the campus and told them I was doing maintenance checks for the ITBE. Note that I didn’t intent to change the configuration of the access point at this moment, but just wanted to determine how students would react making them believe. I used *Netstumbler* to pinpoint the location of the access points and connected my laptop with a serial cable to the access point. In all three cases they let me connect my laptop to the access point with the serial cable. In one case they even offered me a cup of coffee while I was ‘working’.



Figure 43: My 'ITBE id card'

Conclusion

It is not very difficult for an outsider to gain access to the access points and change the configuration. This attack can be detected by the ITBE-staff. It is unknown what the followed procedure by the ITBE-staff is in case of such detection and whether it can be executed quick enough to prevent any harm.

3.3.4.4 Installing Rogue access points

Test goal

To fool users to connect to my own access point and subsequently viewing the unencrypted data stream without their knowledge.

Test procedure

This attack is based on the deployment of an access point (with a strong signal) without the knowledge of the IT staff. Placing this access point provides an easy way for the attacker to capture network traffic, keys and other valuable information.

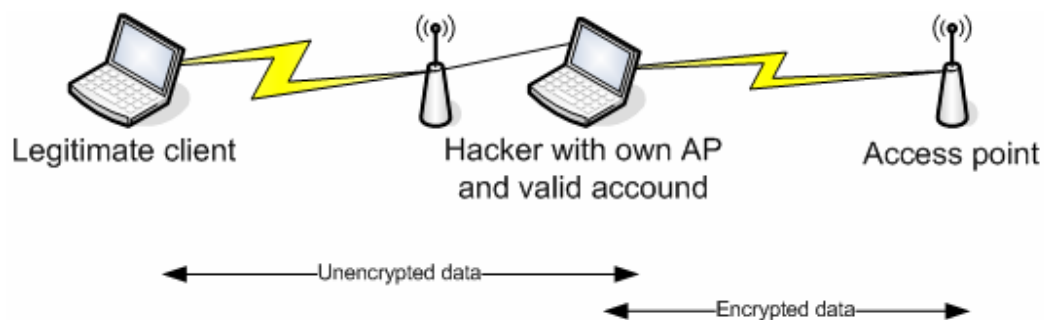


Figure 44: rogue access point

Used hard- and software

For the victims machine I used a windows 2k machine with secure W2 version 2.0.0 and a Linksys WPC54G wireless NIC. The attacker's system had both win 2k and winXP installed. This system contained an Intersil internal wireless NIC. The Software used is Ethereal, DHCP Turbo and Netstumbler 0.4.

Furthermore I used a Cisco Aironet 1200 series access point with IOS firmware. Internet access is required for this test.

Results

I connected the windows 2k system to the legitimate access point with my own account. Next I connected the rogue access point to my laptop. On the rogue access point I set the SSID to "WLAN" and turned WEP encryption on. Having the rogue access point also carry a WEP key lends a good deal of credibility to the attack, and could prevent the rogue device from immediate discovery. A client using windows 2k or windows XP within the range of my access point would now automatically connect to my access point.

In such an attack I would recommend not to place the access point too close to another legitimate access point. Doing so would cause a large amount of reassociations, which could draw undue attention to the fact that a new access point is in the area. Using Netstumbler, I measured the signal strength of the other access point in the area. Using this as a guide, I positioned the rogue access point in a location equidistant between the legitimate access points. This would ensure that the wireless devices could reauthenticate and reassociate with the legitimate access points once the rogue access point had captured their information.

With the rogue access point in place, I let the client system automatically connect to it.

The connection will look as normal as can be seen in Figure 45.

Windows connects automatically to the strongest available signal. In this test, the victim didn't receive any warnings or other indications that the connection was configured in another way as usual. However clicking the "more information" button might conceal our attack to an attentive user.



Figure 45: Linksys settings

All the settings look exactly the same as normal, except for the IP-address (assigned by DHCP Turbo on the hacker's machine). The IP-address here is 192.168.190.57 while all Utwente IP addresses are in the 130.89 range. This difference is caused by the fact that I was using a windows 2k system as a router.

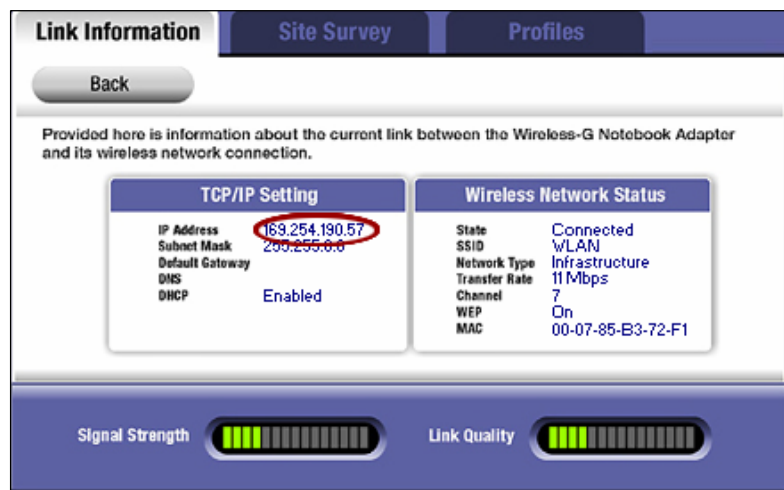


Figure 46: Detailed settings for the Linksys card

For the time of the connection I could capture and analyze the network traffic passing through.

To give the user an IP-address in the 130.89 range I have two options. I can assign an IP-address in the 130.89 range which I expect to be unused to the user myself, or I can use a bridge instead of a router and try to get an IP-address from the Utwente DHCP server. (Note that my access point needs an IP in this range too using this setup. In this case I would have to spoof the MAC-addresses of these devices.)

According to the ITBE staff, the newest version of the secure W2 clients prevents Windows from setting up new connections unnoticed.

Conclusion

The installation of a rogue access point enables an attacker to capture and analyze the network traffic passing through. The chance of detection is negligible.

3.3.4.5 Social engineering

While I was working on this project I received my student ID card, used for identification at exams and similar purposes, in my mailbox. I was slightly surprised about this procedure, because the mailboxes are in a public accessible area. Because of this I could easily pick out three ID-cards from my neighbor's mailboxes. Regrettably the card also contains an image of the owner and therefore not preferred to use.

Test goal

Obtain user credentials by social engineering.

Test procedure and results

I used two social engineering 'techniques' to obtain user credentials: Shoulder surfing and I impersonating someone else.

Shoulder surfing

The first attempt to collect account information was in the University library. Users need their credentials to log into the library systems. This required login paradoxically weakens the protection of the users. It turned out to be very easy to collect credentials from a number of users.

Impersonating another user

I tried to fool the helpdesk (ITBE) playing the role of the student who has accidentally lost his user password and ask for it or a new one. (Of course resetting or changing of the password is not preferred because the actual user will definitely notify this)

Before I could perform this attack I needed some information of another student to 'prove' my identity. I collected the user information below from public available sources including post box with name/student number combinations and online information.

Name:	F.de Wit
Date of birth	19-06-1981
Student number	9902074
Address:	Witbreuksweg 385-108
Phone	053-4895171
background info	TBK

I created a fake email address to confuse the helpdesk employee in the case they wanted to send me the new password by mail. Of course they couldn't send it to my student account since this was the one I lost the password from.

This address is fdewit_99@hotmail.com

Password for this account: *itsmine*

I visited the helpdesk just 10 minutes before they would close the office, so I wouldn't have time to go home to pick up my ID-card in case they would ask. I told them I was on my way home and didn't have any identification on me but really needed my password today. The helpdesk member told me I couldn't change my password without proper authorization. I offered to go home and immediately send an (already prepared) scan of my student ID-card to the helpdesk by mail, and asked if they could send the password in a reply. They refused to do so and told me to come back the next day.

Conclusion

In this case the helpdesk employee took the right decisions, and handled according to the policy. Shoulder surfing is a good way to collect user credentials.

3.3.4.6 Wireless clients

Clients are using the same account information for both the wireless network and reading mail on the wired LAN. Therefore clients can be targeted on both the wired and wireless network to get the credentials that grant access to the WLAN. Most attacks on other users won't be detected by the SNT or ITBE staff since there is no intrusion detection system in place.

Test goal

Collect user credentials from a clients' system or data stream to or from this system.

Test procedure

Username/password information can be stored in Outlook express or some FTP client (used to connect to the Utwente ftp server). Retrieving these passwords would require physical access to the systems and unnecessary annoy these clients. Furthermore, the result of such an attack would depend on the selection of the client. Because of this I performed an ARP attack as described on page 23 against several systems on both the wired and wireless LAN.

Used hard- and software

I used *Cain version 2.5b56* to perform these attacks. This tool allowed me to scan the network for MAC-addresses and execute the ARP poison attack. To minimize the risk of detection the MAC-address can be spoofed with one found in the scan (and therefore registered to another user). Cain has build-in capabilities for detecting MAC-addresses on the (wireless) LAN. Hundreds of addresses where detected in seconds. Each one of these (registered) addresses can be used to spoof your own address and access the LAN. I used Ethereal to analyze the intercepted traffic.

Results

I divided the description into two sections, the first about ARP attacks on the wired LAN and the second about ARP attacks on the WLAN.

ARP attacks on the wired LAN

I decided not to spoof my MAC-address in the first run, so I could see whether there would be any response of the SNT or ITBE staff at all. I looked up the IP addresses of two friends of mine and the one of the Utwente router. I used *Cain* to execute the ARP poisoning attack. To filter unnecessary information from the Ethereal analyzer I added filters based on source and destination IP-address and TCP port for email traffic (110).

The results where surprising. I intercepted a password on both the selected targets within half an hour! See Figure 47 and 48 for the results of these captures. One of them (figure 48 shows the capture) was an Utwente password that could be used for anonymous access the wireless network. Note that Cain itself has a feature to intercept these passwords also.

No.	Time	Source	Destination	Protocol	Info
85	147.	195.121.6.53	130.89.189.247	POP	Response: +OK POP3 service at smtp14.wxs.nl starting
86	147.	195.121.6.53	130.89.189.247	POP	[TCP Retransmission] Response: +OK POP3 service at smtp14.wxs.nl starting
87	147.	130.89.189.247	195.121.6.53	POP	Request: USER chape006
88	147.	130.89.189.247	195.121.6.53	POP	[TCP Retransmission] Request: USER chape006
94	147.	195.121.6.53	130.89.189.247	POP	Response: +OK password required for user chape006
95	147.	195.121.6.53	130.89.189.247	POP	[TCP Retransmission] Response: +OK password required for user chape006
96	147.	130.89.189.247	195.121.6.53	POP	Request: PASS koehand3
97	147.	130.89.189.247	195.121.6.53	POP	[TCP Retransmission] Request: PASS koehand3
06	147.	195.121.6.53	130.89.189.247	POP	Response: +OK Maildrop ready
07	147.	195.121.6.53	130.89.189.247	POP	[TCP Retransmission] Response: +OK Maildrop ready
08	147.	130.89.189.247	195.121.6.53	POP	Request: STAT
09	147.	130.89.189.247	195.121.6.53	POP	[TCP Retransmission] Request: STAT
16	147.	195.121.6.53	130.89.189.247	POP	Response: +OK 0 0
17	147.	195.121.6.53	130.89.189.247	POP	[TCP Retransmission] Response: +OK 0 0
18	147.	130.89.189.247	195.121.6.53	POP	Request: QUIT
19	147.	130.89.189.247	195.121.6.53	POP	[TCP Retransmission] Request: QUIT
22	147.	195.121.6.53	130.89.189.247	POP	Response: +OK
23	147.	195.121.6.53	130.89.189.247	POP	[TCP Retransmission] Response: +OK

Figure 47: First ARP poisoning on the LAN

Credentials from students using webmail are harder to intercept, because the data passing through is encrypted. I didn't get any response of the ITBE or SNT (remember I didn't spoof my MAC address so I shouldn't be too hard to detect).

45	66.2	130.89.1.29	130.89.166.75	POP	Response: +OK Cubic Circle's v1.31 1998/05/13 POP3 ready <63620000a6e8da4
46	66.2	130.89.1.29	130.89.166.75	POP	[TCP Retransmission] Response: +OK Cubic Circle's v1.31 1998/05/13 POP3 r
47	66.2	130.89.166.75	130.89.1.29	POP	Request: USER s
48	66.2	130.89.166.75	130.89.1.29	POP	[TCP Retransmission] Request: USER s
49	66.2	130.89.1.29	130.89.166.75	TCP	pop3 > 1157 [ACK] Seq=77 Ack=16 win=5840 Len=0
50	66.2	130.89.1.29	130.89.166.75	POP	Response: +OK s9909931 selected
51	66.2	130.89.1.29	130.89.166.75	TCP	[TCP Dup ACK 8049#1] pop3 > 1157 [ACK] Seq=77 Ack=16 win=5840 Len=0
52	66.2	130.89.1.29	130.89.166.75	POP	[TCP Retransmission] Response: +OK s selected
53	66.2	130.89.166.75	130.89.1.29	POP	Request: PASS perring8
54	66.2	130.89.166.75	130.89.1.29	POP	[TCP Retransmission] Request: PASS perring8
55	66.2	130.89.1.29	130.89.166.75	TCP	pop3 > 1157 [ACK] Seq=100 Ack=31 win=5840 Len=0
56	66.2	130.89.1.29	130.89.166.75	TCP	[TCP Dup ACK 8060#1] pop3 > 1157 [ACK] Seq=100 Ack=31 win=5840 Len=0
57	67.1	130.89.1.29	130.89.166.75	POP	Response: +OK Congratulations!
58	67.1	130.89.1.29	130.89.166.75	POP	[TCP Retransmission] Response: +OK Congratulations!
59	67.1	130.89.166.75	130.89.1.29	POP	Request: STAT
60	67.1	130.89.166.75	130.89.1.29	POP	[TCP Retransmission] Request: STAT
61	67.1	130.89.1.29	130.89.166.75	TCP	pop3 > 1157 [ACK] Seq=122 Ack=37 win=5840 Len=0
62	67.1	130.89.1.29	130.89.166.75	POP	Response: +OK 5 31953

Figure 48: Retrieving user credentials using ARP spoofing

ARP attacks on the WLAN

ARP attacks on the wireless network are performed in the same way as on the wired LAN. Using the wireless LAN has some pros and cons

Pros ARP attacks on the WLAN:

- Even more anonymity using a spoofed MAC and harvested account
- Credentials are immediately available at the wireless system.

Cons ARP attacks on the WLAN:

- Low bandwidth slows down data traffic and limits the number of targets eavesdropped on at the same time
- Less users 'available' for the attacks
- Attacked users are indeed using their wireless account. This may lead to conflicts when using the credentials at the same time.

Conclusion

ARP attacks are a good way to collect user credentials. These attacks are not detected because no intrusion detection system is in place. (This is confirmed in an interview with the ITBE-staff later in the project).

3.4 Summary

Man-in-the-Middle attacks and Session hijacking doesn't apply to the current implementation.

It is not very difficult for an outsider to gain access to the access points and change the configuration. This attack can be detected by the ITBE-staff. It is unknown what the followed procedure by the ITBE-staff is in case of such detection and whether it can be executed quick enough to prevent any harm.

The installation of a rogue access point enables an attacker to capture and analyze the network traffic passing through. The chance of detection is negligible.

Using the same account for the WLAN as for FTP and email access introduces several possibilities to obtain users credentials. Examples of possible techniques are shoulder surfing and ARP poisoning attacks. ARP poisoning on the wired or WLAN could provide an attacker who possesses an account already additional user credentials for the WLAN. These attacks are not detected because no intrusion detection system is in place.

4 The Utwente security- policy and measures

This chapter describes the management measures concerning the wireless network. Based on the results described in the previous chapters I created a six page questionnaire for the technical staff and talked to members of various departments including the Computer Emergency Response Team. The complete questionnaire is in Dutch and can be found in appendix 6

4.1 SNT (Studenten Net Twente)

The SNT represents the interests of her members for the network facilities offered by the ITBE including WLAN. The SNT is the interlocutor between her members and the ITBE. The SNT supports members, offers information and manuals and settles abuse reports. The helpdesk and abuse department both consists of paid members.

The first acquaintance with the SNT was a little bit earlier as planned. I was disconnected from the WLAN from one moment to the other, and unable to login again. I was a little surprised about this because I didn't start testing for vulnerabilities at that moment yet. When I tried to enter the network I received a "reject" message from the server which indicates that my account was disabled. I visited the helpdesk all the time, but the only thing they could do for me was sending me the error message they retrieved from their system to Google for a solution. A week later another guy at the helpdesk told me they disconnected me because of a virus on my system. I didn't believe a word of what he claimed but since he was very sure I was on the list of disconnected users and could only be reconnected when I removed the virus I searched my system for this virus (which wasn't there of course) and returned to the SNT. This time, the guy working at that moment couldn't find my system on the list of disconnected users. He also couldn't even find any information at all about the other times I complained about my connection too and told me that I should try to Google for a solution as his colleague did two weeks earlier. A week and a half later, I was suddenly connected again. Of course this example doesn't have to be characteristic for all their incident handlings, but it at least demonstrates that there are no clear procedures for incident handling used. .

The SNT website [SNT] doesn't pay much attention to security at all. On their extensive website there is only one small note in the policy that states that commercial or illegal activities like hacking are prohibited.

I asked a member of the SNT abuse department to tell me something about the security of the WLAN and the priority of security incidents for the SNT. It appeared that viruses and SPAM do have the highest priority for the abuse department. No intrusion detection systems (IDS) are used to protect user's systems and no suspicious behavior is investigated before they receive an explicit complaint of a user. T&S a part of ITBE which is the focal point for complaints and security concerning to IT facilities at the university forwards incidents to SNT. The document, describing the incident handling [PRKL] for the ICT-facilities, devotes only 5 lines to the description of the complete procedure for handling of the incident by the SNT.

4.2 ITBE

The ITBE [ITBE] is responsible for the network facilities on the university. The most important issues derived from the interview with the ITBE are enumerated below.

- CERT-UT is the part of ITBE that has the task to coordinate the avoidance and solution of security incidents. The task of CERT-UT is the detection and coordination of the handling of security incidents. CERT-UT also offers advice concerning treats. Their website describes various ways for a user to protect him. This looks as a good initiative, however a closer look reveals the document is made a while ago and at most partly updated ever since. As an example the document describes the distribution of viruses through floppies and contains several dead links.
- The ITBE is aware of the present shortcoming of the GUEST network. A web-proxy will be installed in the near future to improve the protection of this WLAN.
- The ITBE is satisfied with the current implementation of the wireless network.
- With regard to my findings, that were a result of the choice to use the same account in different environments, the ITBE declares they don't expect this to be a problem, and indicate that the current solution is more user friendly in their opinion.
- Incidents based on complaints from users have the same priority as other issues.
- No intrusion detection systems, scans or other preventing measures are used to protect home users on the wired or wireless LAN.
- It looks like the policy is executed based on years of experience of the administrators. With the exception of a dated incomplete document that just gives a general description of the handling of incidents, no policy could be delivered. Guidelines and procedures for the monitoring and control on management and technical measures aren't recorded.
- WLSE is used to monitor and manage access points
- No short term changes on the WLAN are expected
- Users aren't forced to use strong passwords and change them regularly
- The RADIUS system itself is connected directly to the 'unsafe' environment and not protected with a firewall
- The RADIUS server is also used for other applications and services. This can introduce unnecessary vulnerabilities.
- A clean desk policy is in use. There is also a policy for document retention and destruction.

Before the interview I expected that the ITBE-staff would use an IDS and similar systems to keep an eye on the network users. It turned out to be not the case. I also expected that they wouldn't like a student writing stories about the shortcomings of the network and therefore wouldn't supply me with the necessary documentation. This was also a mistakenly assumption. The ITBE-staff was very helpful and interested in the results and recommendations. In this way both parties could benefit from the situation. The most important thing I learned from the interviews was that the security part is just one aspect that plays a role in the final decision. Costs and user-friendliness are at least just as important.

4.3 Summary

The SNT represents the interests of her members for the network facilities offered by the ITBE including WLAN. The SNT is the interlocutor between her members and the ITBE. The SNT supports members, offers information and manuals and settles abuse reports.

The ITBE [ITBE] is responsible for the network facilities on the university. Most important issues derived from an interview with the ITBE concern security and password policy, and documentation of those and other procedures. Furthermore no audits or IDS are used to protect home users preventively.

5 Countermeasures

This chapter describes countermeasures against the attacks described in the chapters before. I also describe the use of (wireless) intrusion detection systems and auditing.

5.1 Countermeasures

5.1.1 Applicability of the countermeasures

The measures described in this chapter are described from a security viewpoint. The goal of a chosen implementation should be to create a network as optimal as possible, not as secure as possible. As an example, writing and observing a security policy is a good thing to do from a security viewpoint. However, administrators already possess this knowledge and might consider this paperwork as a waste of their time. Another example concerns the user-friendliness of the WLAN. From a security viewpoint I would suggest to use different strong passwords for different applications and force the user to change these passwords with a regular interval. Furthermore I would suggest disabling all services a user has by default and let the user activate these if necessary. From the users point of view this would be an undesired situation. In other words the described countermeasures should not implicitly be implemented.

5.1.2 Management Countermeasures

Management countermeasures for securing wireless networks begin with a comprehensive security policy. A security policy, and compliance therewith, is the foundation on which other countermeasures—the operational and technical—are rationalized and implemented. A (WLAN) security policy should be able to do the following:

- Identify who may use WLAN technology in an organization;
- Identify whether Internet access is required;
- Describe who can install access points and other wireless equipment;
- Provide limitations on the location of and physical security for access points;
- Describe the type of information that may be sent over wireless links;
- Define standard security settings for access points;
- Provide guidelines on reporting losses of wireless devices and security incidents;
- Provide guidelines on the use of encryption and key management;
- Define the frequency and scope of security assessments to include access point discovery;
- Describe information classification and handling: to ensure that confidential information is correctly classified as such, and it is secured and disposed of properly. Compliance would result in environment and network information being secured, and not easily available to everybody;
- Describe personnel security: screening new and non employees to ensure that they do not pose a security threat;
- Describe physical security: to secure the facility via sign in procedures, electronic and biometric security devices etc;
- Describe protection from viruses: to secure the systems and information from viruses and Trojans;
- Provide guidelines on information security awareness training and compliance: to ensure that employees are kept informed of threats and counter measures;
- Describe compliance monitoring: to ensure that the security policy is being complied with;
- Describe password policies: standards for secure passwords should be defined;

- Provide guidelines on documentation retention and destruction. For example all confidential information should be disposed of by shredding, not by discarding in the trash or recycle bins.

A good password policy should include information about:

- Not sharing passwords;
- Not writing down passwords;
- Not using default passwords;
- Methods for identifying users for password resets;
- Methods for password delivery;
- Password creation i.e. minimum length, alpha-numeric;
- Securing workstation with a password protected screen saver before leaving a workspace;
- Periodic password change;
- Login failure lockout i.e. account is locked after 3 failed attempts.

Once the policy is documented, it needs to be made easily available to all users and administrators. For the policy to be effective, education must be a regular feature. Some companies require all employees review the policy each year, to acquaint themselves with revisions if any. Next to administrators, also users must be trained on “how to identify information which should be considered confidential, and have a clear understanding of their responsibilities to protect it”.

Next to education, checks on applying of the policy are a requirement. It is generally known that even experienced users as administrators (most time using lots of passwords) regularly use the same weak passwords in for different purposes, even if a password policy is involved. Very little experienced users choose strong passwords in all situations.

As a demonstration, consider the Windows passwords stored (in the *sam file*) on the laptop I borrowed from the University during the project. I assume all other users of this laptop are experienced users since they are all in one way or another connected to the IT department of the faculty.

Of the 12 accounts, at least 11 appeared to be protected with a password build from a basic character set. Several of these weak passwords even contained the usernames, (birth?)days, or had a very small size (less that eight characters).

In this case probably no sensitive information is available on the laptop itself and as far as I know the password doesn't provide access to network or other resources so there is no need for a strong password policy in this case. It is unknown but not impossible that the same passwords are chosen for other accounts as well. Anyway this at least demonstrates the probability ‘normal’ users and employees would choose a weak password without a (forced) password policy.

All users should be trained on how to keep confidential data safe. Therefore it is necessary to get them involved in the security policy. According to SANS, organizations use “some combination of the following: videos, newsletters, brochures, booklets, signs, posters, coffee mugs, pens and pencils, printed computer mouse pads, screensavers, logon banners, notepads, desktop artifacts, T-shirts and stickers”. The important point made, however, is that these things be changed regularly, or the users will lose sight of their meaning.

5.1.3 Operational Countermeasures

Physical security is the most fundamental step for ensuring that only authorized users have access to wireless computer equipment. Physical security combines such measures as access controls, personnel identification, and external boundary protection.

It is important to consider the range of the access point when deciding where to place an access point in a WLAN environment. If the range extends beyond the physical boundaries of the office building walls, the extension creates a security vulnerability. An individual outside of the building, perhaps

“wardriving,” could eavesdrop on network communications by using a wireless device that picks up the RF emanations.

Organizations should use site survey tools to measure the range of access point devices, both inside and outside of the building where the wireless network is located. In addition, organizations should use wireless security assessment tools (e.g., vulnerability assessment) and regularly conduct scheduled security audits.

5.1.4 Technical Countermeasures

Technical countermeasures involve the use of hardware and software solutions to help secure the wireless environment. Software countermeasures include proper access point configurations (i.e., the operational and security settings on an access point), software patches and upgrades, authentication, intrusion detection systems (IDS), and encryption. Hardware solutions include Virtual Private Networks (VPN) and public key infrastructure (PKI)

Software Solutions

Technical countermeasures involving software include properly configuring access points, regularly updating software, implementing authentication and IDS solutions, performing security audits, and adopting effective encryption. These are described in the paragraphs below.

- **Access Point Configuration** - Network administrators need to configure access points in accordance with established security policies and requirements. Properly configuring administrative passwords, encryption settings, reset function, automatic network connection function, Ethernet MAC Access Control Lists (ACL), shared keys, and Simple Network Management Protocol (SNMP) agents will help eliminate many of the vulnerabilities inherent in a vendor’s software default configuration.
 - **Controlling the reset function** - The reset function poses a particular problem because it allows an individual to negate any security settings that administrators have configured in the access point. It does this by returning the access point to its default factory settings. Organizations can detect threats by performing regular security audits. Additionally, reset can be invoked remotely over the management interface on some products.
 - **Changing default passwords** - Each WLAN device comes with its own default settings, some of which inherently contain security vulnerabilities. The administrator password is a prime example. Administrators should change default settings to reflect the agency’s security policy, which should include the requirement for strong administrative passwords.
 - **Establishing proper encryption settings** - Encryption settings should be set for the strongest encryption available in the product.
 - **Changing the SSID** - The SSID of the access point must be changed from the factory default.
 - **Using SNMP** - Some wireless access points use SNMP agents, which allow network management software tools to monitor the status of wireless access points and clients. The first two versions of SNMP, SNMPv1 and SMPv2 support only trivial authentication based on plain-text community strings and, as a result, are fundamentally insecure. SNMPv3, which includes mechanisms to provide strong security are highly recommended. If SNMP is not required on the network, the agency should simply disable SNMP altogether. It is common knowledge that the default SNMP community string that SNMP agents commonly use is the word “public” with assigned “read” or “read and write” privileges. Using this well-known default string leaves devices vulnerable to attack.
- **Personal Firewalls** - Resources on public wireless networks have a higher risk of attack since they generally do not have the same degree of protection as internal resources. Personal firewalls offer some protection against certain attacks.

- **Patches and upgrades** - Vendors generally try to correct known software (and hardware) security vulnerabilities when they have been identified. These corrections come in the form of security patches and upgrades. Network administrators need to regularly check with the vendor to see whether security patches and upgrades are available and apply them as needed. Also, many vendors have “security alert” email lists to advise customers of new security vulnerabilities and attacks. Administrators should sign up for these critical alerts.

5.1.5 Measures against specific attack types

Specific measures against DoS attacks

The upcoming 802.11i standard for advanced security on all 802.11 networks will not prevent the jamming attacks. 802.11i is only a solution for authentication of users and encryption of data.

There is a number of security features used to identify and prevent 802.11 DoS attacks based on flooding or the usage of management frames. These include RF fingerprinting, signature detection, association flood detection, frame rate anomaly detection, rate limiting for 802.11 management frames, and detection of MAC-address spoofing. The net result is that many attacks are prevented, while all attacks are logged and reported to the network manager. These reports typically include the time, the type of attack, the target of the attack, and the approximate physical location of the attack.

Specific measures against ARP attacks

There are several tools that can be used to protect your network from ARP spoofing. These tools, such as *ArpWatch*, will notify an administrator when ARP requests are seen. Another option is to statically define the MAC/IP address definitions. This will prevent the attacker from being able to redefine this information. However, due to the management overhead in statically defining all network adaptors' MAC-address on every router and access point, this solution is rarely implemented.

Intrusion detection systems (IDS) are capable of detecting ARP attacks.

At layer-2: *LBL's Arpwatch* can detect changes in ARP mappings on the local network, such as those caused by *Arpspoof* or *Macof*

Enabling port security on a switch or enforcing static ARP entries for certain hosts helps protect against *Arpspoof* redirection, although both countermeasures can be extremely inconvenient.

Specific measures against sniffing techniques

Next to the use of key rotation or other advanced (expensive) techniques, the only way to protect wireless users from attackers who might be sniffing is to utilize encrypted sessions wherever possible: This includes the use of SSL for e-mail connections, Secure Shell (SSH) instead of telnet, and Secure Copy (SCP) instead of File Transfer Protocol (FTP).

Specific measures against rogue access points

The ease of detecting a rogue access point depends on the sophistication of the intruder.

The easiest way to discover rogue access points would be through the use of *Netstumbler*. However, this would only be true if the rogue access point was deployed as an open system. If it were deployed as a closed system, it would avoid detection through this manner.

Another way to detect rogue access points is through a systematic search of the MAC-addresses on the LAN. The resulting list of MAC addresses can be compared to known access point MACs.

Yet another way to detect and remove rogue access points is by deploying 802.1x authentication throughout your WLAN. Unlike RADIUS authentication that only authenticates the end-user, 802.1x will also require the access point to authenticate itself back to the central server. This solution is not without fault, as a rogue access point could be used to capture 802.1x transactions and enable the intruder to analyze them for potential playback.

Preventing (Physical) Social Engineering Attacks

In order to truly keep trade secrets from escaping the building, some measures are required. Anyone who enters the building should have his/her ID checked *and* verified. No exceptions. Some documents will need to be physically locked in file drawers or other safe storage sites. Other documents may require shredding – especially if they ever go near the dumpster. Also, all magnetic media should be bulk erased. Lock the dumpsters in secure areas that are monitored by security.

Back inside the building, it should go without saying that all machines on the network need to be *well* protected by properly implemented passwords. Screen saver passwords are also recommended. PGP and other encryption programs can be used to encrypt files on hard drives for further security

Access point security recommendations:

- Enable centralized user authentication (RADIUS, TACACS+) for the management interface.
- Choose strong community strings for Simple Network Management Protocol (SNMP) and change them often.
- Consider using SNMP Read Only if your management infrastructure allows it.
- Disable any insecure and nonessential management protocol provided by the manufacturer.
- Utilize secure management protocols, such as Secure Shell Protocol (SSH).
- Limit management traffic to a dedicated wired subnet.
- Isolate management traffic from user traffic and encrypt all management traffic where possible.
- Enable wireless frame encryption where available.
- Physically secure the access point.

5.2 Intrusion Detection Systems (IDS) and monitoring

An intrusion detection system (IDS) is an effective tool for determining whether unauthorized users are attempting to access, have already accessed, or have compromised the network. IDS for WLANs can be host-based, network-based, or hybrid. The hybrid combines features of host- and network-based IDS. A host-based IDS adds a targeted layer of security to particularly vulnerable or essential systems. A hostbased agent is installed on an individual system (e.g., a database server) and monitors audit trails and system logs for suspicious behaviour, such as repeated failed login attempts or changes to file permissions. In some cases, an agent can halt an attack on a system, although a host agent's primary function is to log and analyze events and send alerts. Hostbased systems have an advantage over network-based IDS when encrypted connections (e.g., SSL Web sessions or VPN connections) are involved. Because the agent resides on the component itself, the hostbased system is able to examine the data after it has been decrypted. In contrast, a network-based IDS is not able to decrypt data. Therefore, encrypted network traffic is passed through without investigation.

Organizations should consider implementing a wireless IDS solution that provides the following capabilities:

- Identification of the physical location of wireless devices within the building and surrounding grounds;
- Detection of unauthorized peer-to-peer communications within the wireless network that are not visible to the wired network;
- Analysis of wireless communications and monitoring of the 802.11 RF space and generation of an alarm upon detection of unauthorized configuration changes to wireless devices that violate security policy;
- Detection of and alarming for when a rogue access point goes live within the agency's security perimeter;
- Detection of flooding and disassociation attempts before they successfully compromise the wireless network;
- Provision of centralized monitoring and management features with potential for integration into existing IDS monitoring and reporting software to produce a consolidated view of wireless and wired network security status.

5.3 Auditing

Auditing is by far the most overlooked activity. When deploying any technology Auditing is an activity that should be performed continuously over the lifetime of a wireless network system. Audits are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure it remains secure. A typical audit includes a review of all documentation and procedures, an evaluation of the IT infrastructure and risk assessments.

It is important for organizations to perform regular risk assessments using wireless network analyzers and other tools. Administrators should periodically check within the office building space (and campus) for rogue access points and against other unauthorized access.

Typically, risk assessment involves:

- Determining the likelihood of a specific threat based on historical information and the real-world experience of experts, administrators, and other technical staff;
- Ranking each threat from least likely to most likely;
- Determining the value and criticality of each resource;
- Developing cost-effective methods for mitigating risk.

Most of these risk assessment require administrators to physically move around the building to locate access points and/or determine their security configuration. This type of risk assessment can only provide a snapshot of an organisation's wireless network security stance. IBM Research and the IBM PC Division developed a possible solution for this issue: DWSA.

Distributed Wireless Security Auditor

Distributed Wireless Security Auditor (DWSA) provides an ongoing autonomic assessment of the security configuration of access points in an organisation and reports the physical location of these wireless access points.

Instead of an administrator performing an audit examining the wireless system, DWSA harnesses the power of all the wireless clients on the network. Each client runs a stripped down version of WSA (Wireless Security Auditor) that periodically reports its view of the wireless network to a back-end server in an anonymous fashion. This view consists of all the access points that the client detected along with their security configuration. The back-end server verifies this observation against a list of known and valid access points.

If the server detects an unknown access point or one with a security configuration violation, the server computes the physical location of the offending access point using the signal strength observed by the client and the locations of some known valid access points through a process of tri-lateration. The physical location of the access point together with the violation is then reported to the administrator.

5.4 Summary

Measures to secure the wireless network can be divided into three major categories: management, operational and technical measures. A well documented and available security and password policy, physical security and firewall usage are important examples of such measures. IDS and audits are effective ways to improve the security level.

6 Conclusion, evaluation and recommendations

This chapter starts with a conclusion and evaluation of the found results and project as a whole. I also give recommendations for WLAN usage in several areas, including SOHO networks and the Utwente network as well as suggestions for further projects.

6.1 Conclusion, evaluation and recommendations

During this project I obtained insight in the vulnerabilities of WLAN security, in particular the security of the Utwente WLAN. In this chapter I provide recommendations to remove or mitigate these vulnerabilities. This work provides answers to the questions enumerated in paragraph 1.1 and therefore I may conclude that the main objective of the project is reached.

In general, I didn't stumble across major difficulties during this project. However, familiarize myself with the wireless techniques took more time as expected. I experienced that there is a lot of documentation available about wireless security and it isn't easy to separate the wheat from the chaff. The available documentation is often aged or incomplete. At the beginning of the project I didn't realize that subjects such as legislation issues and social engineering are directly connected to wireless security. However these turned out to be important issues.

I had several meetings with my supervisors during the project which were used to evaluate the progress, the made choices and discuss the results and planning.

I formulated two hypotheses at the beginning of the project. The first hypothesis (paragraph 1.2) was: *Most of the WLAN vulnerabilities today are caused by badly installed systems or already dated hard- or software. Unaware users are the biggest threat to the wireless network.*

This hypothesis is partly confirmed by the results of the wardrive session. Most detected networks were protected using weak protection methods, defaults passwords or no protection at all. Other projects show similar results. The test with the rogue access points also showed that unaware users are a big threat to the network. Because I performed the wardrive session in a residential area only, I can conclude that the hypothesis is true for wireless home and SOHO networks. For these networks I would advice to use PSK-WPA with a strong password, and regularly change this password.

Hotspots don't provide any security at all. Most important recommendation is that you should be aware of this while using a hotspot. Additional recommendations are described in paragraph 2.3.2.

The second hypothesis from paragraph 1.2 was:

The protection of the wireless network of the UT contains vulnerabilities which can be abused with sophisticated techniques. As a result unauthorized access to the network and/or disclosure of sensitive data is possible and therefore the demands of the UT on the WLAN security are not met.

The security of the Utwente WLAN left a good impression. MitM attacks and session hijacking techniques were ineffective. Nevertheless, some other techniques where successful and therefore confirm the hypothesis. Most important demands of the University are “*unique identification of the user*” and “*Identity theft should be impossible*”. An attacker has several options to obtain user credentials and subsequently use these to gain access to the WLAN. This applies especially to attackers who already possess a valid account.

Based on the tests and interviews I would suggest the following improvements for the Utwente WLAN:

- Creating detailed documentation of security guidelines and procedures for employees (ITBE/SNT)
- Perform regular checks on the usage of these policies and guidelines.
- Enforce password policy for users, containing rules for password length and validity
- Install a intrusion detection or intrusion prevention system to protect users' systems.(it is common knowledge that in every company most attacks are performed by employees)
- Explicitly mention the lack of protection on the guest network in the user manual.
- Disable all WLAN accounts by default and activate them on request of the identified user. (Only a small part of all users is using the WLAN).
- Create a procedure for the detection of vulnerable access points and inform users of these access points of the risks and their responsibility for this access point.

Academia and large companies in general usually use VPNs, 802.1x, or WPA solutions. At the moment WPA is the best option.

Banking, government, hospitals and the military shouldn't use WLAN for classified information at all. I recommend the use of VPN or WPA for other purposes in these environments.

Before the interview with the ITBE-staff I expected that the ITBE-staff would use an IDS or similar systems to keep an eye on activities on the WLAN. It turned out to be not the case. I also expected that they weren't in need of a student writing stories about the shortcomings of the network and therefore wouldn't supply me with the necessary documentation. This was also a mistakenly assumption. The ITBE-staff was very helpful and interested in the results and recommendations. In this way both parties could benefit from the situation. The most important thing I learned from the interviews was that the security part is just one aspect that plays a role in the final decision. Costs and user-friendliness are at least just as important.

I remember this project with pleasure. I had a pleasant cooperation with my supervisors. Because the subject appeals to a lot of people, it is a nice subject to tell about. A final plus of this project was that it could be performed in Enschede, which implies that I didn't have to travel over a long distance like during my internship.

6.2 Subjects suggested by the author for further research

I would like to suggest the following subjects for further research.

- 802.11a security issues;
- In depth research on attacks against encryption;
 - o IV/WEP key replay
 - o Frame bit flipping
- WPA vulnerabilities;
- Bluetooth vulnerabilities;
- Investigation of the possibilities to protect data on portable devices;
- UMTS/GPS/GPRS security;
- Possibilities to bypass VLAN traffic diversion;
- Research on the mathematical relation between the preset 802.11 frame size and the time efficiency of WEP cracking;

7 References

Books, Articles, Manuals, Presentations

general

- [1061] 802.11x's elusive security
<http://www-106.ibm.com/developerworks/wireless/library/wi-80211security.html>
- [AB21] WIRELESS SECURITY ARCHIVE
<http://www.ab2m.net/wireless/>
- [ARBA] *An Initial Security Analysis of the IEEE 802.1X Standard*
Professor William Arbaugh and Arunesh Mishra, University of Maryland;
<http://www.cs.umd.edu/~waa/1x.pdf>
- [ARP1] wireless access point and arp poisoning
<http://www.cigitalabs.com/resources/papers/download/arppoison.pdf>
- [BLA1] Wireless LAN Security with 802.1x, EAP-TLS, and PEAP
<http://www.blackhat.com/presentations/win-usa-03/bh-win-03-riley-wireless/bh-win-03-riley.pdf>
- [BORI] Borisov, *Intercepting Mobile Communications: The Insecurity of 802.11*, Berkeley, 2001
<http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>
- [CIS1] The Cisco Aironet 1200 Series
available at: <http://www.cisco.com/en/US/products/hw/wireless/ps430/index.html>
- [COOK] Cookbook WLAN@UT
<http://www.utwente.nl/civ/utnetbasisvoorzieningen/medewerkers/projecten/CookbookWLANatUT/index.html> en presentaties/index.html
<http://www.utwente.nl/itbe/ictinfra/netwerk/WLAN/techniek/cookbook/>
- [DOBB] Dobbesteijn, *What about 802.1X?* Amsterdam, October 2002,
<http://www.surfnet.nl/innovatie/wlan/802.1Xen.pdf>
- [DOMI] *DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots*
http://portal.acm.org/ft_gateway.cfm?id=990077&type=pdf&coll=GUIDE&dl=GUIDE&CFID=28892105&CFTOKEN=93773390
- [DWSA] *DWSA developed jointly by IBM Research and the IBM PC Division.*
<http://www.research.ibm.com/gsal/dwsa/>
- [EDW] *Counter Hack* [Edward Skoudi](#) Prentice Hall PTR | USA Edition | 2001
- [FLIC] *Wireless hacks: 100 Industrial Strength Tips and Tools* , Rob Flickenger,
- [HAMZ] Hamza, *Wireless network security*, May 2003
http://www.ece.umd.edu/class/ents650/Wireless_Security_present.pdf
http://www.ece.umd.edu/class/ents650/Wireless_Security_present.pdf
- [HSV2] *Boingo Bolsters Hotspot Security*
<http://www.astalavista.com/index.php?section=news&cmd=details&newsid=668>
- [KAGA] Kagan, *How Things Work: WLAN Technologies and Security Mechanisms*
http://www.giac.org/practical/GSEC/Anna_Kagan_GSEC.pdf
- [MAXI] Maxim, Merrit and Pollino, *Wireless Security*, Osborne McGraw-Hill, 2003
- [MIC] MIC description
<http://www.linuxsecurity.com/docs/Hack-FAQ/wireless-networks/mic-message-integrity-check.shtml>
- [MICH] Michiels, *Telematics Systems Security*
- [NET1] Hacking the Invisible Network: Insecurities in 802.11x
<http://www.net-security.org/dl/articles/Wireless.pdf>
- [NET1] Wireless LAN Security - What Hackers Know That You Don't
<http://www.netsuds.com/docs/wlansecurity.pdf>
- [OVER] Overbeek, Lindgreen, Spruit, *Informatiebeveiliging onder controle*, Amsterdam, Pearsons Educatieve uitgeverij
- [PAC1] An introduction to ARP spoofing
http://www.packetstormsecurity.com/papers/protocols/intro_to_arp_spoofing.pdf
- [PAU] Paul Dekkers, *Eindverslag 802.1x bij Surfnet.*
<http://www.surfnet.nl/innovatie/wlan/eindverslag-paul.pdf>
- [PILO] *pilot8021x*
<http://www.utwente.nl/wlan/pilot8021x.doc/>
- [PRKL] Procedure klachtafhandeling ICTVoorzieningen (intern document ITBE)
<http://Tensintra.civ.utwente.nl/tns/dbm/files/2687.html>

- [SAN1] Is 802.1X Ready for General Deployment?
<http://www.sans.org/rr/papers/9/709.pdf>
- [SUR1] Authentication and Authorisation for (W)LAN using 802.1X
<http://www.surfnet.nl/innovatie/wlan/>
- [SUR2] Mogelijkheden om een IEEE 802.1x netwerk te beveiligen.
<http://www.surfnet.nl/innovatie/wlan/wlanxsoverview.shtml>
- [TEC1] The war over 802.11x security
<http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2783681,00.html>
- [UTG] Handleiding SNT gebruik GUEST network
http://www.utwente.nl/itbe/werkplekondersteuning/voorlichting_helpdesk/handleidingen/alle_handleidingen/wlan_guest_winxp.doc/index.html
- [UTWL] Informatie over het WLAN op de UT
<http://www.utwente.nl/civ/utnetbasisvoorzieningen/medewerkers/projecten/CookbookWLANatUT/wlanatut.doc/index.html>
- [WEP1] Scott Fluhrer, Itsik Mantin, and Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4
http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf
- [WEP2] Practical Exploitation of RC4 weaknesses in WEP environments
<http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt>
- [WIDZ] WIDZ - The Wireless Intrusion detection system
http://www.loud-fat-bloke.co.uk/articles/widz_design.pdf
- [WIF1] Deploying 802.1X for WLANs: EAP Types
<http://www.wi-fiplanet.com/tutorials/article.php/3075481>
- [WIF11] Linux-hackers kunnen WiFi-bandbreedte stelen
<http://www.tweakers.net/nieuws/32834>
- [WPA1] Wireless News: Aruba gets WPA2 certified
http://www.tomsnetworking.com/News_story_793.php
- [WPA1] Wifi Protected Access
http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf
- [WPA2] Wifi Protected Access
<http://www.tomsnetworking.com/Sections-article50-page1.php>
- [WPA3] Wifi security
http://www.wifialliance.com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf
- [WR11] Detecting Wireless LAN MAC Address Spoofing
<http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf>
- [XFOR] Active wireless protection
<http://documents.iss.net/whitepapers/ActiveWirelessProtection.pdf>

Hotspot information and Bluetooth vulnerabilities

- [HSV1] News item about Hotspot vulnerabilities
http://weblog.pcmweb.nl/2004/03/hotspot_event_2_2.html
- [BT4] Integralis Security Advisory: Multiple Vendor Mobile Phone Bluetooth DoS
http://www.integralis.co.uk/about_us/press_releases/2004/120504SA.html
- [BT5] Integralis Security Advisory: Mobile Phone Anonymous Bluetooth Access Vulnerability (CHAOS-Attack)
http://www.integralis.co.uk/about_us/press_releases/2004/260304.html
- [BT6] Integralis Overview - Vulnerable Mobile Phones (12.05.04)
http://www.integralis.co.uk/about_us/press_releases/2004/120504OM.html
- [WLUS] Presentatie Sander SMit (UT) over WLAN@UT security
<http://www.cisco.com/global/NL/events/endusers/pdf/Pres4a.pdf>

Social engineering

- [SE01] Methods of Hacking: Social Engineering Rick Nelson
<http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html>
- [SE02] Arthurs, Wendy: "A Proactive Defence to Social Engineering," SANS Institute, August 2, 2001.
<http://www.sans.org/infosecFAQ/social/defence.htm>
- [SE03] Berg, Al: "Cracking a Social Engineer," *LAN Times*, Nov. 6, 1995.
http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html
- [SE04] Fine, Naomi: "A World-Class Confidential Information and Intellectual Property Protection Strategy", Pro-Tec Data, 1998. <http://www.pro-tecdata.com/articles/world-class.html>
- [SE05] Harl: "People Hacking: The Psychology of Social Engineering" Text of Harl's Talk at Access All Areas III, March 7, 1997. <http://packetstorm.decepticons.org/docs/social-engineering/aaatalk.html>

- [SE06] Nelson, Rick: "Methods of Hacking: Social Engineering," the Institute for Systems Research, University of Maryland <http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html>
- [SE07] Stevens, George: "Enhancing Defenses Against Social Engineering" SANS Institute, March 26, 2001 http://www.sans.org/infosecFAQ/social/defense_social.htm
- [SE08] Verizon "PBX Social Engineering Scam" 2000 http://www.bellatlantic.com/security/fraud/pbx_scam.htm

Tools

- [AIRC] *Aircrack: 802.11 sniffer and WEP key cracker for Windows and Linux.*
<http://www.cr0.net:8040/code/network/aircrack/>
- [AIRJ] *Airjack, packet injection tool*
<http://sourceforge.net/projects/airjack/>
- [AIRO] *Airopeek NX*
http://www.wildpackets.com/products/airopeek_nx
- [AIRS] *Airsnort homepage*
<http://airsnort.sourceforge.net/> and <http://airsnort.shmoo.com/>
- [CAIN] *Cain and Abel*
<http://www.oxid.it/>
- [DSNI] *Dsniff*
<http://www.monkey.org/~dugsong/dsniff/>
- [ETCH] *Etherchange*
<http://ntsecurity.nu/toolbox/etherchange/>
- [ETHE] *Ethereal*
<http://www.ethereal.com>
- [ETTE] *Ettercap*
<http://ettercap.sourceforge.net/>
- [KISM] *Kismet*
<http://www.kismetwireless.net/>
- [KMAC] *K-mac*
<http://www.packetstormsecurity.org/Win/indexdate.html>
- [LNSS] *LANguard Network Security Scanner*
<http://www.gfi.com/lannetscan/>
- [MAMA] *Mac Makeup*
<http://www.gorlani.com/publicprj/macmakeup/macmakeup.asp>
- [MSNM] *MS network monitor*
<http://support.microsoft.com/default.aspx?scid=kb;en-us;148942&sd=tech>
- [NETS] *Netstumbler*
<http://www.netstumbler.com/>
- [SMAC] *Smac MAC spoofer*
<http://www.klcconsulting.net/smac/>
- [SNPR] *Sniffer Pro*
<http://www.networkassociates.com/us/products/home.htm>
- [TCPD] *TCPdump: network analyzer*
<http://www.tcpdump.org/>
- [WEPC] *WEPCrack homepage*
<http://wepcrack.sourceforge.net/>
- [WEPL] *WepLab*
<http://sourceforge.net/projects/weplab>
- [WEPW] *Wepwedgie*
<http://sourceforge.net/projects/wepwedgie/>

- [1MAN] *Tools installation manuals*
http://www.geekspeed.net/~beetle/download/wifi_dog.html
- [LINK] *LinkFerret Off-Line WEP Decrypter*
<http://www.linkferret.ws/download/download.htm>

Websites

- [HS01] *Boingo (hotspot provider)*
<http://www.boingo.com/>
- [HS02] *Wayport (hotspot provider)*
<http://www.wayport.com/>
- [HS03] *Stsn (hotspot provider)*
<http://www.stsn.com/>
- [HS05] *Hotspot locations*
<http://www.hotspot.nl>
- [HS06] *Hotspot locations*
<http://www.vindhspot.nl/>
- [HS07] *Swisscom homepage; a hotspot provider*
<http://www.swisscom-eurospot.com/>
- [HS08] *Information about KPN hotspots*
<https://portal.hotspotsvankpn.com>
- [HS09] *Viawia, another hotspot provider*
<http://www.viawia.nl/>
- [HS10] *T-Mobile; a large hotspot provider in the Netherlands*
www.t-mobile.nl/hotspot
- [HS11] *Mobilander, another hotspot provider*
<http://www.mobilander.nl/>
- [HS12] *WinQ; another hotspot provider*
<http://www.winq.com/>
- [HS4] *Prorail, this organisation provides wireless Internet on Hengelo and Enschede train station.*
<http://www.prorail.nl/ProRail>
- [ITBE] *Dienst Informatietechnologie, Bibliotheek en Educatie*
www.utwente.nl/itbe
- [SNT] *Studenten Net Twente*
www.snt.utwente.nl
- [TKI1] *TKIP description*
<http://www.tech-faq.com/wireless-networks/kip-temporal-key-integrity-protocol.shtml>
- [TKI2] *802.11 Security Series :Part II: The Temporal Key Integrity Protocol (TKIP)*
http://cache-www.intel.com/cd/00/00/01/77/17769_80211_part2.pdf
- [VPN] *VPN description*
<http://www.uninett.no/wlan/vpn.html>
- [WAR] *This site maps all known access point in the Netherlands.*
<http://www.wardrivemap.nl/>

RFC, Standards

- [2382-8] ISO/IEC international standard 2382-8 *Information technology Vocabulary, part 8 Security*

8 Glossary

<i>active wiretapping</i>	Wiretapping with the purpose to modify or insert data
<i>access control list</i>	A list of entities, together with their access rights, which are authorized to have access to a resource
<i>authentication</i>	The act of verifying the claimed identity of an entity
<i>breach</i>	The successful circumvention or disablement of some element of computer security, with or without detection, which if carried to completion, could result in a penetration of the data processing system
<i>brute-force-attack</i>	A trial-and-error attempt to violate computer security by trying possible values of passwords or keys
<i>ciphertext</i>	Data produced through the use of encryption, the semantic content of which is not available without the use of cryptographic techniques
<i>computer security</i>	The protection of data and resources from accidental or malicious acts, usually by taking appropriate actions
<i>compromise</i>	A violation of the security policy of a data processing system in which programs or data may have been modified, destroyed, or made available to unauthorized entities
<i>cryptanalysis</i>	An attempt to decipher a code or find a key by systematic means
<i>decryption</i>	The process of obtaining the original data from a ciphertext
<i>denial of service</i>	The prevention of authorized access to resources or delaying of time critical operations
<i>DHCP</i>	Dynamic Host Configuration Protocol : The protocol used to assign Internet Protocol (IP) addresses to all nodes on the network
<i>disclosure</i>	A violation of the security policy of a data processing system in which data have been made available to unauthorized entities
<i>encryption</i>	The cryptographic transformation of data
<i>flooding</i>	Insertion of a large volume of data resulting in denial of service
<i>flaw</i>	An error or weakness that allows protections mechanisms to be bypassed
<i>initialisation vector</i>	value used in defining the starting point of an encryption process
<i>monitor mode</i>	A wifi specific way of sniffing, which allows you to listen to all traffic without associating to any network
<i>mutual authentication</i>	Entity authentication which provides both entities with assurance of each others identity
<i>passive wiretapping</i>	Wiretapping limited to obtaining data
<i>physical security</i>	The measures used to provide physical protection of resources against deliberate and accidental threats
<i>plaintext</i>	unencrypted information
<i>promiscuous mode</i>	A NIC mode that allows you to sniff traffic on the network you are connected to. Not to be mixed up with monitor mode.
<i>Risk</i>	describes the potential loss measured against vulnerabilities
<i>security audit</i>	An independent review and examination of data processing system records and activities in order to test for adequacy of data processing system controls, to ensure compliance with established security policy and operational procedures, to detect breaches in security , and to recommend any indicated changes in control, security policy and procedures
<i>security policy</i>	A document that states in writing how a company plans to protect the company's physical and IT assets
<i>spoofing</i>	“IP spoofing” refers to sending a network packet that appears to come from a source other than its actual source
<i>threat</i>	A potential violation of security
<i>vulnerability</i>	see “flaw”
<i>war dialing</i>	A technique in the 1980s and '90s by which a computer would repeatedly dial a number (usually to a crowded modem pool) in an attempt to gain access
<i>wardriving</i>	An activity consisting of driving around with a laptop in one's vehicle, detecting wireless networks
<i>wired equivalent privacy (WEP)</i>	Wired Equivalent Privacy is a security protocol, specified in the IEEE WiFi standard, 802.11, that is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN

8.1 Acronyms and Abbreviations

1G	1 st Generation
3DES	Triple DES
AAA	Authentication, Authorization and Accountancy
ACL	Access Control Lists
ADSL	Asynchronous Digital Subscriber Line
AES	Advanced Encryption Standard
AP	Access Point
APS	Application Protocol Systems
ARP	Address Resolution Protocol
ATM	Automatic Teller Machine
BS	Base station
BSS	Basic Service Set
BSSID	Basic Service Set Identification
CA	Certificate Authority
CDP	Cisco Discovery Protocol
CERT	Computer Emergency Response Team
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CoS	Class of Service
CRC	Cyclic Redundancy Check
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DES	Data Encryption Standard
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Server
DoS	Denial of Service
DWSA	Distributed Wireless Security Auditor
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
EAP-TLS	EAP with Transport Layer Security
EAP-TTLS	EAP with Tunneled Transport Layer Security
ESP	Enterprise Service Provider
ESS	Extended Service Set
FMS	Fluhrer, Mantin, and Shamir
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer (SSL)
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technologies
ICV	Integrity Check Value
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

IOS	Internetworking Operating System
IP	Internet Protocol Interactive Proof
IPSec	IP Security
IPX	Internetwork Packet Exchange
ISO	International Standardization Organization
ISP	Internet Service Provider
IT	Information Technology
ITBE	InformatieTechnologie, Bibliotheek en Educatie
IV	Initialization Vector
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAP	Lightweight Directory Access Protocol
LEAP	Cisco's Lightweight EAP
LED	Light Emitting Diode
MAC	Medium Access Control
MD5	Message Digest 5
MIC	Message Integrity Check
MITM	Man in the middle (attack)
MitM	Man in the Middle (attack)
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
NAS	Network Access Server
NAT	Network Address Translation
NIC	Network Interface Card
OS	Operating System
OSA	Open System Authentication
OSI	Open Systems Interconnection
OTP	One Time Password
OUI	Organizationally Unique Identifier(MAC)
PAE	Port Access Entity
PAP	Password Authentication Protocol
PBX	Private Branch eXchange (a private telephone network used within an organization)
PCMCIA	PC Memory Card Interface Adapter
PDF	Portable Document Format
PEAP	Protected EAP
PKI	Public Key Infrastructure
PKI	Public Key Infrastructure
POP	Post Office Protocol
PPP	Point to Point Protocol
PPTP	Point-to-Point Tunneling Protocol (Microsoft)
PRNG	PseudoRandom Number Generator
PSK	Pre-Shared Key
RADIUS	Remote Access Dial-in User Service
RC4	Rivest Cipher 4
RF	Radio Frequency
RFC	Request For Comment
SIM	Subscriber Identity Module
SKA	Shared Key Authentication
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Attachment Point header (layer 2 encapsulation header)

SNMP	Simple Network Management Protocol
SNT	Studenten Net Twente
SOHO	Small Office Home Office
SQL	Structured Query Language
SSH	Secure SHell
SSID	Service Set IDentifier
SSL	Secure Socket layer
T&S	Telecommunicatie en Systeembeheer
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide Area Network
WBP	Wet Bescherming Persoonsgegevens
WEP	Wired Equivalent Privacy
WIFI	Wireless Fidelity
WISP	Wireless Internet Service Provider
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WLSE	Wireless LAN Solution Engine
WPA	WiFi Protected Access

Appendices

Appendix 1: Eisen en wensen aan het WLAN mbt de beveiliging

E7.8:

De af luisterbeveiliging en gebruikersauthenticatie van het wireless verkeer moet adequaat geregeld zijn (specificatie: zie hierboven).

De aangeboden apparatuur kan dit regelen door verschillende technieken:
<ul style="list-style-type: none">• 128-bits WEP• EAP-Cisco (LEAP)• EAP-TLS• TKIP → uitbreiding op WEP en gebouwd op basis van de, in ontwikkeling zijnde, beveiligingsstandaard 802.11i (MIC en Key Hashing). Cisco heeft hierop nog Keyrotation als extra toegevoegd.• Eind dit jaar ook PEAP (Protected EAP). Ondersteunt onder andere OTP (One Time Password) en Token card oplossingen.
E7.9:
<i>Volledige implementatie van IEEE 802.1x (Port based network access control)</i>
Cisco Aironet 1200 ondersteunt volledig IEEE 802.1x in de vorm van EAP-Cisco en EAP-TLS.
E7.10:
<i>Dynamische WEP-keys tussen client en access point.</i>
EAP-Cisco, EAP-TLS en eind 2002 PEAP en PEAP met OTP. Daarnaast nog additioneel Broadcast Key Rotation.
E7.11:
<i>APs moeten beschermd zijn tegen niet-geautoriseerde toegang (bijv. SSH, ACL).</i>
Op dit moment user database per access point en kan bestuurd worden met WLSE (Wireless LAN Solution Engine). SSH wordt ondersteund in het komende nieuwe release (september/oktober).

O7.4:

Het CIV ziet graag van de inschrijver zijn visie hoe oneigenlijk gebruik van het wireless netwerk op de UT kan worden tegen gegaan.

In deze beschrijving dienen de volgende onderwerpen aan de orde te komen:

- IEEE 802.1x;
- EAP, EAP-TLS, EAP-TTLS;
- Dynamische WEP-key toewijzing;
- Virtual Private Network (VPN)
- Versleutelen van data
- Authenticatie servers, RADIUS, MS-Active Directory
- Noodzakelijke extra software op de clients.

Oneigenlijk gebruik van wireless netwerken kan op meerdere manieren opgelost worden. In grote lijnen is wireless netwerk security op de volgende manieren toe te passen:

- Static WEP keying
- EAP/802.1x gebaseerde oplossingen
- VPN oplossingen

De eerste oplossing blijkt in de praktijk te weinig netwerk security te bieden en zal ook niet verder besproken worden in dit gedeelte.

EAP/802.1x oplossingen zijn voor campus omgevingen goed toe te passen en bovendien schaalbaar.

Zoals bij antwoord W7.8 besproken biedt de, op EAP gebaseerde, EAP-Cisco (LEAP) oplossing een grote toegevoegde waarde om de volgende redenen:

1. Vereist wederzijdse Authenticatie tussen gebruiker en Radius server.

Creëert dynamische WEP keys per sessie, met daarnaast de mogelijkheid om de key na een bepaalde (instelbare) tijd te laten vernieuwen.

Op deze oplossing wordt voor extra data integrity TKIP toegepast. Hierin worden MIC en Per Packet Keying toegepast welke op de drafyt standaard 802.11i is gebaseerd.

Aditioneel op TKIP past Cisco ook broadcast key rotation toe, zodat deze statische key moeilijk wordt om te achterhalen.

Het versleutelen van data gebeurt door middel van zogenaamde 'Cipher Streams' welke bestaan uit een dynamische WEP key en een ge-hashte IV. Op deze manier zal er per pakket een andere sleutel gebruikt worden.

Om EAP Cisco toe te kunnen passen dient men een Radius server te gebruiken die voor deze mogelijkheden ingericht is zoals Cisco Secure ACS. Deze Radius server kan men koppelen aan b.v. Active Directory (op basis van b.v.LDAP), daarnaast kan iedere ODBC (Open DataBase Connectivity) welke MS-CHAP ondersteund worden toegepast. Op deze manier kan Single Signon worden gerealiseerd.

EAP/LEAP regelt Authenticatie op basis van UserID/Password. EAP TLS regelt Authenticatie op basis van PKI oplossingen. EAP TLS is ontwikkeld door Microsoft en wordt nu alleen nog ondersteund in Windows XP. De Wireless oplossing hier gepresenteerd ondersteund EAP TLS.

Aangezien EAP TTLS nog in het vroege stadium draft is, zijn hier nog geen echte toepasbare oplossingen voor. Cisco zal in de toekomst zeker deze standaard gaan ondersteunen.

Voor LEAP heeft men alleen client software nodig op de gebruikers PC.

De bovengenoemde oplossingen zijn goed toepasbaar voor lokale/campus WLANs. Maar indien WLAN wil gaan toepassen op plekken buiten de campus, dan wordt het gebruik van VPN geadviseerd.

Om een VPN verbinding op te kunnen zetten heeft men een VPN concentrator of gateway nodig. Aan de gebruikers zijde heeft men een additionele VPN client nodig.

De Authenticatie voor de VPN toegang kan men laten regelen door een Radius server of door de VPN gateway zelf.

Een product wat goed toepasbaar is b.v. IBM WirelessGateway. Deze gateway verzorgt de VPN connecties voor vele netwerk omgevingen:




































- GPRS
- UMTS
- GSM
- WAP
- ADSL
- Etc.

Een groot voordeel van deze VPN GateWay is dat men networking roaming kan toepassen zonder sessie verlies. Dit betekent dan men b.v. van Wired omgeving over kan gaan naar een wireless omgeving zonder dat er sessie verlies optreedt. Door gebruik van VPN's kan men b.v. veilige sessies opzetten vanaf b.v. Public WLANs (zoals vliegvelden).

Appendix 2: Basisconfiguratie acces point UT WLAN

Hostname	Gebaseerd op het gebouw, kamer en wall outlet
SSID	(zie VLAN configuratie)
RoI	Root Access Point
Optimize Radio Network	Throughput
Ensure Compatibility With	Non-Aironet 802.11
Speed	Auto (100BaseT / Full-Duplex)
Optimize Ethernet for	Performance
Allow Broadcast SSID to Associate	Yes
Enable World Mode	Yes
Kanaal	1, 6 en 11 (Nog nader te bepalen per AP)
Vermogen	Nog nader te bepalen per AP
Configuration Server Protocol	MAC based static DHCP
Default IP Address	Default laten
Default IP Subnet Mask	Default laten
Default Gateway	IP adres van de default router en eventuele andere routes
DNS Configuratie	Configuratie komt uit de DHCP server (niet configureren op Access Point)
MAC Address	Vastleggen om in DHCP server een "vast" adres te reserveren
Protocol Filtering	Niet gebruiken
MAC Filtering	Niet gebruiken
Network Time Protocol	DNS-naam NTP server (ntp.utwente.nl) en timezone (GMT + 01 :00)
Cisco Discovery Protocol	Alleen op ethernet configureren

Appendix 3: Wardriving

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal
 000B5FD7F1A2	WLAN		1	11 Mbps	Cisco	AP	WEP	13	-87
 000B5FD01056	WLAN		6	11 Mbps	Cisco	AP	WEP	13	-87
 000B5FD7F1F6	WLAN		6	11 Mbps	Cisco	AP	WEP	18	-78
 000B5FD0105A	WLAN		1	11 Mbps	Cisco	AP	WEP	17	-82
 000DBC683201	WLAN-TI		3	11 Mbps	Cisco	AP	WEP		-84
 000B5FD0106E	WLAN		1	11 Mbps	Cisco	AP	WEP	9	-91
 000B5FD7F1CC	WLAN		6	11 Mbps	Cisco	AP	WEP	15	-79
 000B5FD0106B	WLAN		6	11 Mbps	Cisco	AP	WEP		-81
 00022D074398	quadapt		10	11 Mbps	Proxim (...)	AP	WEP		-83
 000B5FD01033	WLAN		1+	11 Mbps	Cisco	AP	WEP	17	-76
 000DEDC30C69	WLAN-TI		4	11 Mbps	Cisco	AP	WEP		-87
 000E83612430	WLAN-TI		10	11 Mbps	Cisco	AP	WEP		-69
 000DED901F4A	WLAN-TI		13	11 Mbps	Cisco	AP	WEP	12	-75
 000B5FE7B9C6	WLAN		11	11 Mbps	Cisco	AP	WEP	22	-78
 00022D747257	TI4GB		6	11 Mbps	Proxim (...)	AP	WEP		-69
 000DED901CFF	WLAN-TI		8	11 Mbps	Cisco	AP	WEP	13	-66
 000B5FD7F218	WLAN		1*	11 Mbps	Cisco	AP	WEP	34	-63
 00022D747EFE	TI4GA		5	11 Mbps	Proxim (...)	AP	WEP		-81
 000E8388E263	WLAN-TI		2	11 Mbps	Cisco	AP	WEP	14	-71
 000DBC683223	WLAN-TI		13	11 Mbps	Cisco	AP	WEP		-77
 000B5FD7F221	WLAN		11	11 Mbps	Cisco	AP	WEP	20	-80
 000E83ED9D3B	WLAN-TI		4	11 Mbps	Cisco	AP	WEP		-76
 000B5FE246F6	WLAN		6	11 Mbps	Cisco	AP	WEP	15	-85
 000DBC683405	WLAN-TI		3	11 Mbps	Cisco	AP	WEP		-82
 000B5FE246D7	WLAN		1	11 Mbps	Cisco	AP	WEP	12	-88
 000B5FE246B9	WLAN		11	11 Mbps	Cisco	AP	WEP	20	-80
 000B5FE246DA	WLAN		11	11 Mbps	Cisco	AP	WEP	22	-78
 000B5FD0106D	WLAN		1	11 Mbps	Cisco	AP	WEP	21	-75
 000B5FE246F7	WLAN		6	11 Mbps	Cisco	AP	WEP	23	-75
 000B5FD7F233	WLAN		6+	11 Mbps	Cisco	AP	WEP	13	-64
 000B5FD7F21A	WLAN		11	11 Mbps	Cisco	AP	WEP	25	-75
 000B5FD7F211	WLAN		1	11 Mbps	Cisco	AP	WEP	17	-83
 000B5FE246E3	WLAN		1	11 Mbps	Cisco	AP	WEP	17	-83
 000B5FBCC0F0	WLAN		6	11 Mbps	Cisco	AP	WEP	22	-78
 000B5FD00D25	WLAN		6	11 Mbps	Cisco	AP	WEP	17	-77

When I leave the campus, I found a lot access points without encryption enabled.

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
0050FCD54656	haghuis		1	11 Mbps	Edimax	AP	WEP	13	-87
00C049A632F5	PontusWireless		10	22 Mbps	US Rob...	AP	WEP	22	-78
0060B3019DDC	Enschede		6	54 Mbps	Z-Com	AP	WEP	15	-84
000CF60333E4	Sitecom		10+	11 Mbps		AP	WEP	25	-74
000B5FD010F5	WLAN		6	11 Mbps	Cisco	AP	WEP	11	-89
0040965C5CE6			13	11 Mbps	Cisco	AP		19	-80
0040965972F4			6	11 Mbps	Cisco	AP		8	-86
000D6572C349	ProRail		1	11 Mbps	Cisco	AP		14	-84
0040965B4603			1	11 Mbps	Cisco	AP			-87
004096427DE1			3	11 Mbps	Cisco	AP		9	-83
004096313634			7	11 Mbps	Cisco	AP		12	-81
004096300220			13	11 Mbps	Cisco	AP		15	-81
00022D292A8D			1	11 Mbps	Proxim (...)	AP	WEP		-89

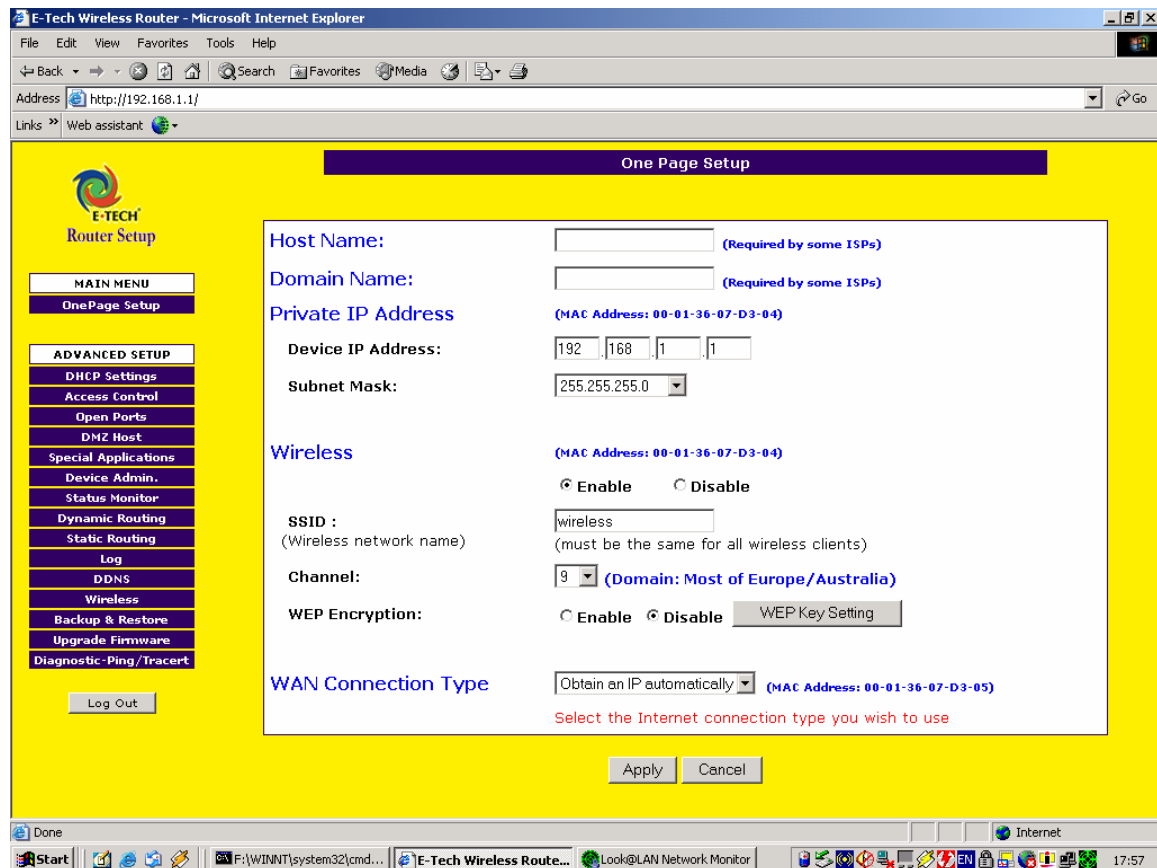
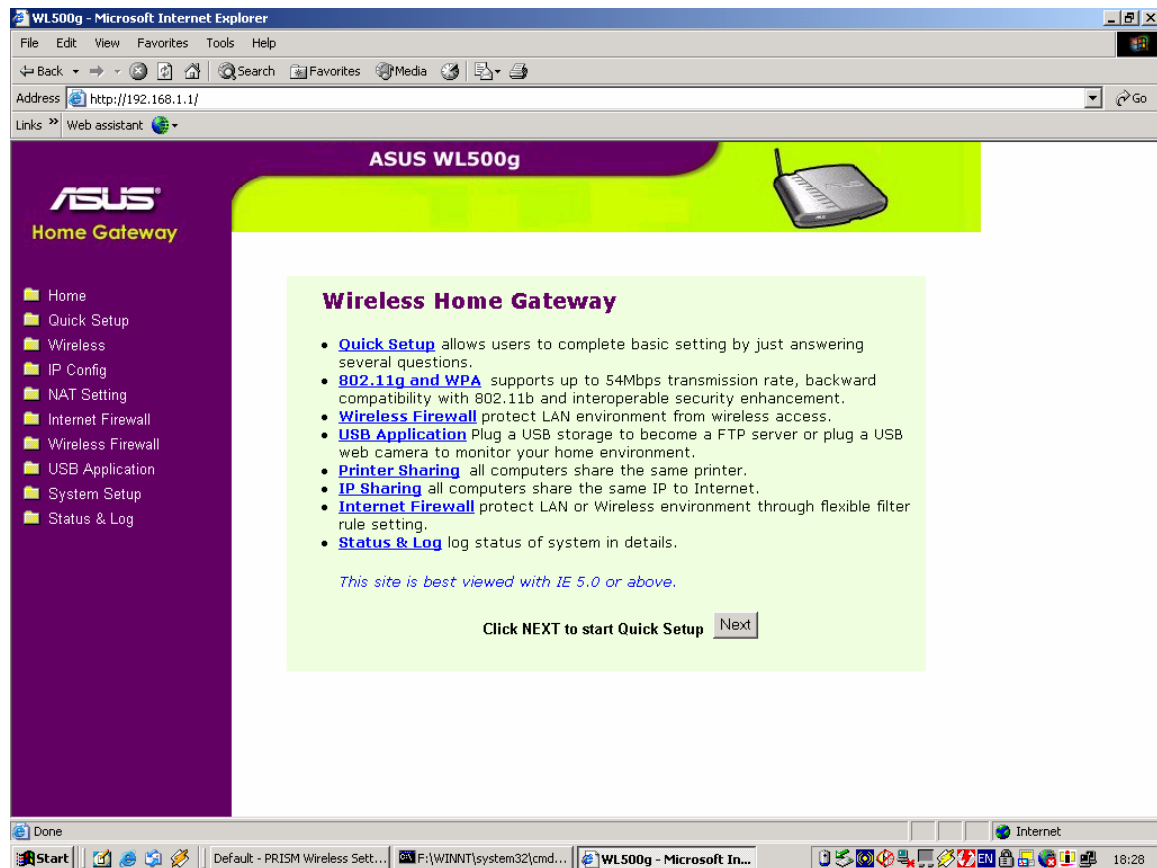
All three NS stations (Enschede, Drienerloo and Hengelo) have APs with SSID 'Prorail' and no WEP enabled. After associating with this network I was redirected to a logon screen. After a few guesses the username/password combination 'test/test' allows network access.

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
00028AA99454	tsunami		2	11 Mbps	Ambit	AP	WEP		-87
0060B301ADF2	Sitecom		6	54 Mbps	Z-Com	AP			-90
000DED2ECE2B	ProRail		11	11 Mbps	Cisco	AP			-82
000F662508FB	linksys		11	54 Mbps	Linksys	AP			-81
0010E7F5D1E1	Enschede_Oost.##		1	11 Mbps	Breeze...	AP			-89
000DBC25EFF5	ProRail		6	11 Mbps	Cisco	AP			-86
000D659BAD07	ProRail		1	11 Mbps	Cisco	AP			-76

Not just private persons neglect to enable encryption on their network.

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+
000D88068D38	default		6	22 Mbps	D-Link	AP	WEP		-88
0060B38A77EF	habels63		6	11 Mbps	Z-Com	AP			-78
0060B318DEA5	cc7957-a		6	11 Mbps	Z-Com	AP			-72
00409635CBB1	tsunami		7	11 Mbps	Cisco	AP			-86
00A0C55D3A8E			1	11 Mbps	Zyxel	AP			-70
00A0C55D3A8D			1	11 Mbps	Zyxel	AP			-61
000D549BCC9A	3Com		11	54 Mbps	3Com	AP			-71
004096436513			10	2 Mbps	Cisco	AP	WEP		-77
0010E7F57162	Hartman_Enschede.##		7	11 Mbps	Breeze...	AP			-90
0060B39926EC	MEDION		6	54 Mbps	Z-Com	AP	WEP		-86
0010E7B5015C	Hartman_Boekelo.\$\$		13	11 Mbps	Breeze...	AP			-81
000D54A02DF3			1	54 Mbps	3Com	AP	WEP		-84
000625F9D3FE	SkeltOr WLAN		11	11 Mbps	Linksys	AP			-79
00032F1D7F3C	default		6	54 Mbps	GST (Li...	AP			-75
000F6645DB6F	lakerink		11	54 Mbps	Linksys	AP	WEP		-75
000625F9CBDE	linksys		11	11 Mbps	Linksys	AP			-78
0004E2AB8A50	FLATNET ROUTER		6	54 Mbps	SMC	AP			-84

Appendix 4: Examples of detected AP's with default passwords



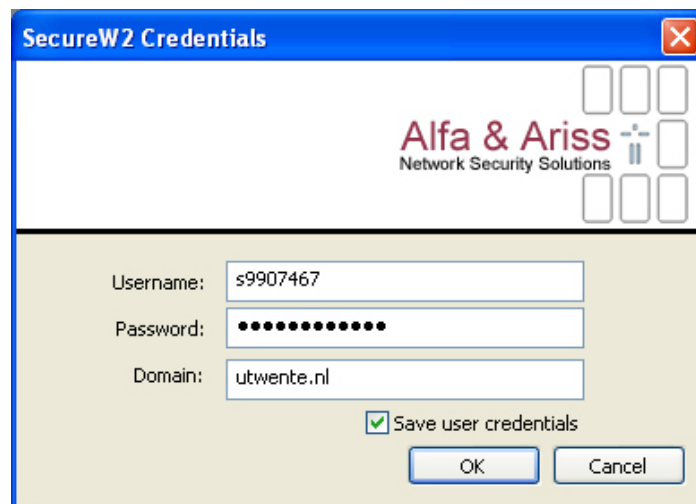
Appendix 5: Authentication procedure on the 802.1X network.

Most students will use the Secure W2 client to connect to the wireless network. This client handles the authentication to the network.

If the option "Use computer credentials" in the client is not selected, you will be prompted a user setup screen on establishing the connection. In the bottom right corner an "Information pop-up" will appear



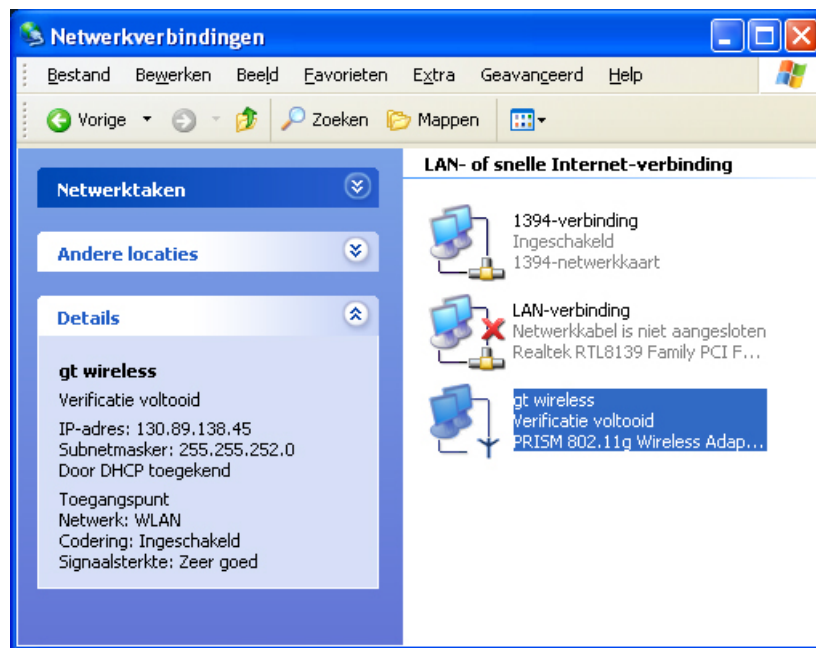
When the user clicks on the "Information pop-up" the user setup screen will appear.



If the SecureW2 client is configured, Windows will start the authentication process. You can follow the authentication process if you select wireless network from the network connection configuration screen. On the bottom left in the details window you will see "verification completed" if the connection is set up correctly. The computer also should obtain an IP address.



If you selected the option "Verify server certificate" in the "Connection setup" tab the first time you authenticate an "Unknown Server" pop-up will appear in the bottom right corner. If you click on this pop-up the following will appear:



This will show the hierarchy of the unknown server. With the option "View Certificate" you can verify the certificate. Before you can connect, all certificates should be verified. To trust a certificate it needs to be installed on the local computer.

Appendix 6: Vragen aan het ITBE

Op basis van resultaten van het onderzoek zijn onderstaande vragen opgesteld. Deze vragen zijn voorgelegd aan en besproken met een tweetal medewerkers van het ITBE. De resultaten hiervan heb ik gebruikt voor de evaluatie van het WLAN@UT onderdeel van het project en tevens om een eventueel advies met betrekking tot de case study “WLAN@UT” te formuleren. De vragen zijn opgedeeld in een zestal onderwerpen.

De meeste vragen worden vooraf gegaan door een veronderstelling. Indien deze veronderstelling onjuist is, was het de bedoeling dat dit ook werd aangegeven.

Onderstaande informatie is deels gebaseerd op het WLAN@UT ‘cookbook’
[<http://www.utwente.nl/wlan/cookbook.doc>]

1. Eisen en wensen volgens het ‘cookbook’

Eis 7.8 uit het ‘cookbook’ luidt: “*De af luisterbeveiliging en gebruikersauthenticatie van het wireless verkeer moet adequaat geregeld zijn*”. Aanvullend worden er in een beschikbare presentatie (<http://www.cisco.com/global/NL/events/endusers/pdf/Pres4a.pdf>) onder andere de volgende eisen gesteld:

- a) Unieke identificatie van de gebruiker.
- b) Onmogelijkheid om identiteit over te nemen.
- c) Eenvoudig beheerbaar.
- d) Gastgebruik moet eenvoudig mogelijk zijn.

Een deel van de vragen is gebaseerd op de boven genoemde documentatie.

- 1.1. Wat is de correctheid en volledigheid op het moment van deze documenten? Zijn er ondertussen aanpassingen aan het netwerk, aangepaste of aanvullende eisen of andere punten waarop de documentatie gedateerd is?
Voldoet aan gestelde eisen. Het GUEST netwerk is open maar wordt binnenkort afgeschermd door een web-proxy
- 1.2. Hoe schat de geïnterviewde in dat de UT op dit moment aan de gestelde eisen voldoet?
Voldoet aan de gestelde eisen
- 1.3. Op welke manier moet “adequaat” in eis 7.8 uit het Cookbook geïnterpreteerd worden? Geld dit voor af luisteren door buitenstaanders of ook voor andere gebruikers?
De beveiligingsnivo moet overeenstemmen met de risico’s die UT overheeft die voortkomen bij eventueel af luisteren

Voor de toegang tot het WLAN wordt gebruik gemaakt van de accountgegevens van de LDAP server die ook gebruikt wordt voor onder authenticatie voor andere zaken als email en FTP. Door met iemand over zijn schouder mee te kijken bij inloggen in de bieb of met bijvoorbeeld een ARP poisoning aanval het verkeer op het vaste netwerk te onderscheppen kunnen account gegevens verkregen worden die toegang geven tot het WLAN. Zelfs gebruikers die helemaal niet van het bestaan van het WLAN afweten hebben ‘automatisch’ een account tot het WLAN die op daarmee ook misbruikt zou kunnen worden.

- 1.4. Waarom is er gekozen voor een koppeling van deze gegevens en niet een aparte database opgezet voor WLAN gebruikers?
Provisioning en je wilt de gebruiker niet opzadelen met lijsten passwords niet gebruikersvriendelijk.

- 1.5. Vind de geïnterviewde dat dit een goede keuze gelet op de eis a) en b) hierboven?
[Voor wlan gebruik JA.](#)
In een gesprek met een medewerker van het SNT kwam naar voren dat ‘aanvallen’ op het WLAN geen prioriteit hebben zolang er niet duidelijke klachten komen van bijvoorbeeld een andere gebruiker.
- 1.6. Welke prioriteit heeft de beveiliging tegen ‘aanvallen’ (en daarmee ook detectie hiervan en afhandeling van incidenten) ten opzichte van bijvoorbeeld het verhelpen van problemen of de bestrijding van virussen bij het ITBE?
[Hoge prioriteit. Systemen die gedetecteerd worden of waarvan we abuse klachten krijgen worden in quarantaine gezet](#)
- 1.7. Vindt de geïnterviewde dat aan de bij 1.6 gestelde zaken de juiste prioriteit is toegekend?
[Ja](#)
- 1.8. Zijn er eerdere beveiligingstests uitgevoerd, en zijn er hierbij zwakheden in de beveiliging vastgesteld die niet gewenst zijn gezien het beleid?
[Ja, Diverse onderzoeken op TTLS. Met sniffers gekeken en ook de berichtgevingen over het protocollen zijn goed.](#)
[Nee, er zijn nog geen zwakheden geconstateerd](#)
- 1.8.1. Zoja, welke zwakheden zijn dit? Zijn er hierna aanpassingen doorgevoerd en in dat geval wat zijn deze aanpassingen?
[<ruimte voor reactie>](#)
- 1.8.2. Zijn er op andere wijze als door middel van tests zwakheden in de huidige implementatie aan het licht gekomen en zijn er hier al beschikbare oplossingen voor voorhanden of toegepast?
[Het gebruik van EAP-TTLS wordt nog niet ondersteund door alle systemen zoals PALM. Oplossing is een andere protocol te kiezen \(PEAP\)](#)

2. Beleid

Ik heb geen informatie kunnen vinden over het gebruik van een security- of wachtwoordbeleid.

- 2.1. Hoe zien dit beleid eruit en wat zijn hierin de verschillen met het beleid betreffende het (vaste) campusnetwerk? Hierbij denk ik onder andere aan:
- Het vernietigen en opslag van vertrouwelijke gegevens als accountinformatie
 - Het resetten en versturen van vertrouwelijke gegevens als accountinformatie
 - Het vaststellen van een beleid voor gebruikers zoals het aansluiten van WLAN apparaten
 - Het bepalen van de minimale fysieke beveiliging van de access points
 - Het opzetten van richtlijnen voor het afhandelen van verdwenen hardware en security incidenten
 - Het uitvoeren van audits en gebruik van een IDS systeem
 - Richtlijnen voor de keuze en geldigheidsduur van wachtwoorden van gebruikers

[Hier moet meer aandacht aan geschonken worden.](#)

- 2.2. Wie maakt dit beleid en op welke manier wordt er bepaald of er aan dit beleid wordt voldaan?

[ITBE in samenspraak met gebruikersgroepen en surfnet](#)

- 2.3. Welke waarde hecht de geïnterviewde aan het gebruik en regelmatig herzien van dit beleid?

[Waardevol](#)

3. Structuur,beheer en taakverdeling

Het WLAN is toegankelijk vanuit de verschillende faculteiten. Tevens kan er in de stad en op de campus ook verbinding worden gemaakt met het netwerk. Deze ‘subnetwerken’ zouden per locatie, maar ook vanuit een centraal punt beheerd kunnen worden. Tevens zijn er verschillende VLAN’s (Volgens het Cookbook een “GUEST”, “WLAN” en twee commerciële VLAN’s). Verschillende organisaties, diensten en personen zoals het ITBE,SNT, CERT-UT en abuse diensten van zowel ITBE als SNT spelen een rol in de beveiliging van het WLAN.

- 3.1. Wat zijn de verschillende onderdelen van het WLAN (verschillende VLAN’s en “subnetwerken”)? En hoe zijn deze met elkaar verbonden (Alle in dezelfde IP range, verschillende rechten etc)
[8 vlans met eigen subnets. Ieder subnet heeft zijn policies en afschermingen](#)
- 3.2. Hoe is het beheer van deze onderdelen verdeeld? Wat voor zaken zijn centraal geregeld en welke zaken worden uitbesteed? (bijvoorbeeld aan de faculteiten), Zijn er naast het ITBE, CERT-UT en SNT nog derden die een rol spelen met betrekking tot de beveiliging van het WLAN?
[Alleen ITBE, cert-UT en SNT zijn onderdelen van ITBE. Beveiliging wordt in samenspraak met gebruikers en o,a surfnet vest gesteld](#)
- 3.3. In geval van een opdeling van de beheerstaken, hoe is de samenwerking tussen de verantwoordelijken geregeld? (bijvoorbeeld in geval van een incident)
[Goed geregeld](#)
- 3.4. Wie zijn er belast met het detecteren en afhandelen van incidenten? (zie ook 6)
[ITBE-T&S](#)
- 3.5. Wat vindt de geïnterviewde van de gekozen taakverdeling?
[Mag meer aandacht aan gegeven worden](#)
- 3.6. Er is een netwerk voor gastgebruik dat slechts registratie van het MAC adres vereist en een WLAN voor studenten en medewerkers waarbij gebruik gemaakt wordt van de 802.1x technologie. Zijn er nog andere onderdelen van het netwerk(bijvoorbeeld in de faculteiten, of een commercieel deel zoals aangegeven in het ontwerp) en op welke manier is de beveiliging op dat deel gerealiseerd? (zie ook vraag 4.9)
[Momenteel nog geen onderscheid. Technisch is eenvoudig om gebruikersgroepen te scheiden en beveiligingstechnieken te hanteren. Dit staat er aan te komen.](#)
- 3.7. Op welke wijze worden de access point’s beheerd? (Cisco WLSE, SNMP, SSH)
[WLSE, SMTP,WEB](#)
- 3.8. De proxyserver is gekoppeld aan een drietal user databases waarvan een van de UT zelf. Betekend dit dat de UT afhankelijk is van goed account beheer van de andere twee instanties? (m.a.w. kan een gebruiker met een surfnet account ook hier inloggen?)
[Ja dat klopt, via eduroam \[www.eduroam.nl\]\(http://www.eduroam.nl\)](#)

4. Beveiliging

- 4.1. Hoe schat de geïnterviewde de kans op (geslaagde) ‘aanvallen’ op het draadloze netwerk in?
[Als je bedoeld het af luisteren van data is de kans zeer beperkt \(WEP-key rotation 20 minuten\). Het password te sniffen is bijna onmogelijk \(3Des\)](#)
- 4.2. In het WLAN@UT project is gekozen om gebruik te maken van de 802.1x standaard waarmee al een aanzienlijk niveau van veiligheid kan worden gecreëerd, wat zijn

hiernaast de maatregelen die de UT heeft genomen met betrekking tot de beveiliging? (IDS, audits, gebruikersovereenkomsten, monitoren access points, gebruikersbeleid)
[Audit, minitoring, data analyse, beleid](#)

- 4.3. Welke informatie wordt er van de gebruikers opgeslagen (Internetgebruik, foutmeldingen, dataverkeer)? Wat gebeurt er met deze informatie en op welke wijze zijn deze loggegevens beveiligd?

[IPadres, ethernetadres, accesspoint. Wordt gebruikt voor abuse. Data staat afgeschermd.](#)

- 4.4. Hoe is de keuze voor deze standaard tot stand gekomen? Is er in het verleden een afweging gemaakt tussen verschillende alternatieven? Welke rol heeft de beveiliging gespeeld bij de uiteindelijke keuze?

[Innovatie project, waren één van de eerste die 802.1x en TTLS grootschalig gebruiken. Keuze van 802.1x tov VPN is dat 802.1x veel schaalbaarder is en geen single point of failure heeft](#)

Van de access points is er een Vxworks en een IOS versie in omloop. Volgens mijn informatie is het de bedoeling dat op termijn alle access points voorzien worden van IOS firmware.

- 4.5. Op welke termijn gaat dit gebeuren en wat is de belangrijkste reden voor deze aanpassing?

[Ik denk volgens jaar. Ontwikkelingen gebeuren op IOS. Ook de 802.11g is alleen verkrijgbaar voor IOS](#)

Uit een van de tests blijkt dat de access points(IOS versie) eenvoudig zijn te resetten door een gebruiker. Hiermee kunnen de instellingen naar keuze worden ingesteld.

- 4.6. Om het netwerk niet onnodig te verstoren is in de test niet vastgesteld of het resetten van de access points daadwerkelijk mogelijkheden oplevert. Krijgt een access point dat is gereset een IP adres toegewezen van de DHCP server en heeft een gebruiker via dit access point direct toegang tot het netwerk? (met of zonder authenticatie)

[De access point is te resetten echter de configuratie is dan gewist.](#)

- 4.7. Welke mogelijkheden worden er gebruikt om aanpassingen in de configuratie van een access point te detecteren en wat is de procedure na zo'n detectie? (en hoe snel kan deze procedure afgewerkt worden)

[WLSE doet dat en signaleert verschillen en geeft ook melding van geresette devices](#)

Bij het testen van het access point, waarbij deze op een vaste campusnet aansluiting werd aangesloten had er binnen korte tijd een nietsvermoedende andere gebruiker via mijn access point verbinding gemaakt met het LAN. Deze gebruiker had hier duidelijk geen weet van want er werd vervolgens langere tijd gebruik gemaakt van de aansluiting. Duidelijk is dat van deze gebruiker het netwerkverkeer eenvoudig kon worden onderschept / aangepast. Bij een klein detectie rondje op de campus werd een aantal malen een access point gedetecteerd met een ander SSID dan "WLAN", mogelijk zijn dit ook zogenaamde rogue access points die op het LAN zijn aangesloten. In dat geval introduceren deze veiligheidsrisico's voor gebruikers en ondermijnen in mijn visie hiermee eis 7.8 van het Cookbook zoals deze in onderdeel 1 gesteld is.

- 4.8. Er zijn verschillende methoden om deze access points te detecteren. Ook kan hierover in een gebruikersovereenkomst iets worden vastgelegd. Wat is het beleid met betrekking tot zogenaamde 'rogue access points'?

[Staat nog op de actie lijst om uit te voeren. Wat jij hierboven beschrijft is alleen mogelijk als je toegang hebt en de secrets hebt van de radiusserver. Als je die niet hebt kunnen gebruikers geen toegang krijgen tot je accesspoint. De secure_UT client die gebruikt wordt voorkomt gebruiker dat die associereren met rogue accesspoints.](#)

Voor aanmelden op het GUEST VLAN is slechts de registratie van het MAC adres nodig. Dit kan echter nauwelijks als een vorm van beveiliging worden gezien. Volgens de SNT handleiding http://www.snt.utwente.nl/handleidingen/windows_2k_xp/wlan_guest_xp_nl.php wordt er geen versleuteling gebruikt voor dit VLAN en lijkt het erop dat er een aparte IP range wordt toegewezen. (IP: 130.89.140.136 / SN:255.255.255.192)

- 4.9. Welke eisen zijn er met betrekking tot beveiliging en privacy van de gebruiker van het GUEST en andere in vraag 3.1 genoemde VLAN's?
[Alleen mac-registratie. Maar wordt binenkort afgesloten door een soort web-proxy. Het guest netwerk is nodig geweest om aanloop problemen met 802.1x te voorkomen](#)
- 4.10. Op welke wijze worden de gebruikers van het GUEST (en eventueel andere aanwezige netwerken) geattendeerd op de afwezigheid van een sterke beveiliging?
[Staat in de handleiding.](#)

5. Incidenten

Incidenten worden afgehandeld door CERT-UT. Deze hanteren een vaste procedure voor het afhandelen van incidenten. De eerste stap in het detecteren van een incident zou een melding van een gebruiker kunnen zijn. Als ik echter op de webpagina over CERT-UT kijk tref ik een dode link aan als ik een incident zou willen melden:

http://www.utwente.nl/itbe/ictinfra/netwerk/beveiliging/New%20content%20link.whlink/procedure_melden_securityincide.html

Het document blijkt (na zoeken via google) te zijn verplaatst naar

http://www.utwente.nl/itbe/ictinfra/beveiliging/DH_Abuse.doc/

- 5.1. Hoeveel incidenten als hackpogingen en scans komen er gemiddeld voor?
[Weet ik niet](#)
- 5.2. Wat is over het algemeen de aanleiding tot een incident? (melding, detectie)
[Weet ik niet](#)
- 5.3. Wat is het beleid en de procedure bij incidenten? Wat vindt de geïnterviewde van dit beleid en deze procedure?
[Meldt aan abuse](#)
- 5.4. Wat zijn er in het verleden voor incidenten geweest naast updates en virussen en op welke wijze zijn deze afgehandeld?
[Weet ik niet](#)
- 5.5. Op welke wijze wordt het gewicht van een incident vastgesteld?
[Weet ik niet](#)

6. De toekomst

Draadloze technologie veroudert snel. Dit geldt ook voor de beveiliging. WPA en 802.1i bieden oplossingen voor een aantal van de kwetsbaarheden die in een 802.1x implementatie kunnen voorkomen.

- 6.1. Zijn er in de toekomst aanpassingen aan (onderdelen van) het WLAN gewenst/te verwachten die betrekking hebben op de beveiliging?
[Ja, 802.11i /e/f/s](#)
- 6.2. Zijn er naar inzicht van de geïnterviewde mogelijke verbeteringen aan het WLAN (met betrekking tot de beveiliging) en daarbij behorende beleid en organisatiestructuur aan te brengen?
[Ja, beleid moet aangescherpt worden](#)
- 6.3. Zijn de bij 6.2 genoemde verbeteringen ook noodzakelijk volgens de geïnterviewde.
[Ja, beleid](#)

Appendix 7: Opdrachtomschrijving afstudeeropdracht

Beveiliging van draadloze netwerken (802.1).

Draadloze netwerken zijn een snel veranderende technologie, waarbij de beveiliging ervan een belangrijk aspect speelt. Het doel van dit onderzoek is duidelijk beeld te krijgen van de huidige ontwikkelingen en tekortkomingen op het gebied van de beveiliging van draadloze netwerken, inzicht te krijgen in het woud van technologieën en beschikbare producten en mogelijk aanbevelingen te doen voor gebruik van draadloze netwerken in de verschillende toepassingsgebieden.

Gebruik van de 802.1x technologie wordt vaak genoemd als (een van) de meest veilige (beschikbare) en schaalbare oplossing voor WLAN's en deze technologie wordt daarom in het bijzonder in het onderzoek bekeken. Ook de UT maakt voor haar netwerk van deze technologie gebruik. De beveiliging van dit draadloze netwerk zal als een testcase onderzocht worden. In het onderzoek komen onder andere de volgende aspecten aan de orde:

1. Beschrijving van de verschillende beveiligingsmethoden voor WLAN's waaronder een hoofdstuk over state-of-the-art oplossingen en verwachtingen voor de toekomst.
2. Beschrijving van aanvalstechnieken en –tools om wlans te hacken
3. Experimenten met aanvallen en beveiligen van netwerken die gebruik maken van verschillende beschikbare beveiligingsmogelijkheden.
4. Aanbevelingen doen voor het veilig inrichten van een WLAN. Hierbij is er te denken aan verschillende scenario's (home, academia)